Concise Explanation of Japanese Patent Application, Laid-Open Publication No. H10-198636

INT. CL.[6]: G06F 15/00
17/60
H04L 9/32
H04M 11/08
H04Q 7/38

PUBLICATION DATE: July 31, 1998

TITLE	SYSTEM AND METHOD FOR PERSONAL AUTHENTICATION
APPLICATION NO.	H09-3420
FILING DATE	January 13, 1997
APPLICANT(S)	NRI & NCC CO LTD
INVENTOR(S)	KENTARO FUJIMOTO

[Abstract]
[Problem to be solved] To provide an authentication technology which does not excessively complicate authentication information held by authenticated member users and does not force on member users too many operations than before.

[Solution] A personal authentication system comprises: member data reading means for reading member data (for example, the address or the domicile of a member user); area data obtaining means for obtaining from a PHS carrier (PP) area data (D2) of a PHS terminal device (20) owned by a member; processing means for determining whether area data (D2) matches member data; and output means, when as a result of a determination of the processing means area data matches member data, for producing an output for allowing a user to continue to receive services from a service provider (AA), and when area data does not match member data, for producing an output for preventing a user from receiving services from a service provider (AA).

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention relates to a personal authentication system and a personal authentication method, and specifically to a system and a method for improving the accuracy of an authentication performed in the time of a transaction using electronic means such as on-line communications or a credit card.

[0002]

[Prior Art] So far, when a contract or a transaction is made using electronic means, a person using electronic means is authenticated on the basis of a personal identification code or a password. For example, in an on-line service (or Internet communications), to make a transaction between an on-line service member and an on-line service provider, an on-line service member sends application information using a personal computer and a telephone line, and a computer system provided in an on-line service provider receives the application information. In such a case, to check the authenticity of the on-line service member, the following method is used so far.

[0003] In advance, PC users make a service contract with an on-line service provider, and the provider determines a member ID number and a password and notifies the users of them. The provider, when receiving an access request from a user, requests the user to enter a pre-registered member ID number and password. When the user enters a member ID number and a password, the provider checks them against authorized member information recorded in the provider. When they match the authorized member information, the provider identifies the user as an authorized member user. The provider assumes order information sent during the communication to be information sent by the authorized member user, and accepts the order information.

[0004] Also, to check the authenticity of authorized contractor more strictly, the provider limits a time period when a user is allowed to enter a member ID number and a password or, when a user mistakenly enter them more than predetermined times, assumes the user to be unauthorized user and terminate the connection from the user. As a result, unauthorized users are precluded.

[0005]

[Problem to be Solved by the Invention] However, the above methods for precluding unauthorized users are rendered ineffective, for example, if a hacker breaks into a transmission gate or a modem of a computer of an authorized member user to obtain the member ID number and the password. Pre-assigned member ID numbers and passwords, if any other person knows them by some means, becomes ineffective as means for authentication.

[0006] To prevent hackers from illegally obtaining member ID numbers and passwords, there used a method of encoding communications between authorized member users and a provider to ensure the security of the communications. However, no matter how advanced and complicated means for preventing illegal obtainments of passwords, etc. may become, the means can not be the ultimate solution against hackers who develop more advanced illegal obtainment means.

[0007] This type of incident has occurred when using banking cards or credit cards. Since an authorized member user often uses for his/her password the last four digits of his/her or his/her close relative's birthday or telephone number not to forget it, it is relatively easy for misusers of passwords to guess such a password. As a result, they can obtain goods illegally.

[0008] A problem to be solved by the present invention is to provide an authentication technology which does not excessively complicate authentication information held by authenticated member users and does not force on member users too many operations than before. An object of the inventions according to Claims 1 to 3, and 9 is to provide a personal authentication system which does not excessively complicate authentication information held by authenticated member users and does not force on member users too many operations than before.

[0009] An object of the invention according to Claim 4 is to provide a personal authentication system which makes it possible to preclude unauthorized users by putting them at a disadvantage. An object of the inventions according to Claims 5 and 10 is to provide a personal authentication method which does not excessively complicate authentication information held by

authenticated member users and does not force on member users too many operations than before.

[0010] An object of the inventions according to Claims 6 and 7 is to provide a personal authentication system which does not excessively complicate authentication information held by authenticated credit card members and does not force on card members too many operations than before. An object of the inventions according to Claim 8 is to provide a personal authentication method which does not excessively complicate authentication information held by authenticated credit card members and does not force on card members too many operations than before.

[0011] To solve the above-mentioned problems, the applicants provides the inventions according to Claims 1 to 10. In the present invention, it is assumed that each authorized member user of the system owns a PHS terminal device, a beeper, or a mobile phone, and that each authorized member user always has a PHS terminal device, etc. at hand. In the personal authentication system and method according to Claims 1 to 8, location information of a PHS terminal device is obtained from a PHS carrier; on the basis of the location information, a location of a person who makes a contract or transaction using electronic means is identified; and if a connection point does not match the location information of the PHS terminal device, the use of the electronic means is determined to be unauthorized.

[0012] In the personal authentication system and method according to Claims 9 and 10, not only a PHS terminal device but also a beeper or a common mobile phone can be used, and whether the use of electronic means is unauthorized is determined based on the presence or absence of a call.

(Claim 1) The invention claimed in Claim 1 is a personal authentication system for authenticating a user, when the user accesses a computer owned by a service provider (for example, on-line service provider AA) providing services using information and communication technology, the personal authentication system comprising: member data storing means for storing member data; member data reading means for reading member data (for example, the address or the domicile of a member user); area data obtaining means for obtaining from a PHS carrier (PP) area data (D2) of a PHS terminal device (20) owned by a member user; processing means for determining whether area data (D2) matches member data; and output means, when as a result of a determination of the processing means area data matches member data, for producing an output for allowing a user to continue to receive services from a service provider (AA),and when area data does not match member data, for producing an output for preventing a user from receiving services from a service provider (AA).

(Definitions of Terms) The "member user" is a member who is authorized to utilize a personal authentication system according to the present invention, and who has completed a registration to a service provider operating the system (for example, on-line service provider (AA), a bank (BB) which issues cash cards, or a credit card company (CC)). The "member user" does not include a shop (C1) having a contract with a credit card company (CC) to make credit cards usable for shopping in the shop (C1).

[0013] To receive services from a service provider, a member user needs connecting means (10). The connecting means (10) is, for example, means for transmitting "communication signals" necessary for communication with a service provider. When the system is applied to an on-line service, connecting means refers to hardware such as a personal computer (12) and a modem (13) and software such as communication software and a password. When the system is applied to transactions by cash cards (15) or credit cards (17), connecting means refers to software such as a card itself (15, 17), data stored in the card (15, 17), and a personal identification code. A cash dispenser (16) for cash cards (15) of a bank or a card reader (18) provided in a shop (C1) having a contract with a credit card company (CC) is a part of "connecting means (10)".

[0014] The "member data" is data pre-stored in a database of a service provider, such as addresses or domiciles, or telephone numbers of member users. The "member data storing means" refers to not only a storage device pre-storing data but also a device for storing data received during communication. When the personal authentication system of the present

invention is applied to an on-line service, the "member data" refers to connection point data (D1) at the time when a member user starts communication with a service provider using connecting means (10) (for example, on-line communication devices such as personal computer 12 and modem 13). The "connection point data (D1)", since it refers to the address or the domicile of an on-line service member, is registered in an on-line service provider (AA), and is stored in a member data database of the on-line service provider (AA). In a case where the connection point data (D1) is read at the time of a connection, if a member user goes out with on-line service communication devices and establishes communication in a place other than the address or the domicile of the member user, the personal authentication system of the present invention works effectively.

[0015] When the system is applied to transactions by cash cards (15) or credit cards (17), member data refers to "connection point data (D1)", namely the location of a shop where a contract or a transaction is made by a cash card (15) or a credit card (17). In such a case, "connection point data (D1)", which corresponds to member data, is registered in a computer center (BB) managed by a bank or a card company (CC), and stored in a database. Also, "connection point data (D1)" is transmitted from a cash dispenser of a bank branch or a card reader (18) of a shop (C2) to a computer center (BB) or a card company (CC).

[0016] The "area data (D2)" refers to the location of a PHS base station (for example, P1) to which a PHS terminal device (20) can connect. Data received by a PHS base station (for example, P1) is used as area data D2. Usually, a PHS terminal device (20) sends and receives a base station ID to/from a PHS base station (P1) via radio waves periodically. A service provider (AA) operating the system obtains area data D2, which is identified based on a base station ID, from a PHS carrier (PP) via a PHS base station (P1).

[0017] When the system is applied to an on-line service, and as shown in Fig. 3 a member user uses on-line services by connecting a PHS terminal device (20) to a modem (13) of a personal computer (12), "area data" refers to the location of a PHS base station (P3) to which the PHS terminal device (20) connects. The "processing means" includes a device, when "member data" and "area data" are simple data, for interpreting and collating both data. For example, as shown in Fig. 1, if area data (D2) can be obtained from a plurality of PHS base stations (P1, P2), it is determined with correcting means whether the area data (D2) matches member data.

[0018] The "output produced when area data does not match member data" usually refers to an output for terminating communication to prevent the continuation of communication or a transaction. The output may be an output for putting an unauthorized user at a disadvantage when the user continues communication, such as data for rewriting data stored in a credit card to make the card unusable. In addition to produce such a output, outputting means may informs an authorized member of the possibility of a misuse via a trusted institution.

[0019] In the personal authentication system according to Claim 1, the following operations are performed. When a member user starts communication with a service provider (AA), the personal authentication system according to the present invention reads member data of the member user with member data reading means. The service provider (AA) obtains from a PHS carrier (PP) area data (D2) of a PHS terminal device 20 owned by the member user with area data obtaining means. The service provider (AA) determines with processing means whether the area data (D2) matches member data pre-recorded in storing means.

[0020] If the member user has the PHS terminal device (20) at hand, the processing means determines that the area data (D2) matches the member data. In such a case, the personal authentication system of the present invention determines that the member user is an authorized member user, and he/she is allowed to continue to receive services from the service provider (AA) by outputting means.

[0021] When the processing means determines that the member data does not match the area data (D2), the personal authentication system of the present invention determines that the member user is not an authorized member user. Consequently, the member user is prevented from receiving services from the service provider (AA) by the outputting means. This is because,

when the member user does not have at hand a PHS terminal device 20 owned by an authorized member user, the access by the member user is very likely to be an unauthorized one.

[0022] As described above, to enable the personal authentication of the present invention, all a member user has to do is to have his/her PHS terminal device 20 at hand. This does not become a burden a member user because a user of a PHS terminal device (20) usually has his/her PHS terminal device (20) at hand.

(Claim 2) The invention claimed in Claim 2, where the invention claimed in Claim 1 is limited to an on-line service, is characterized in that a service provider refers to an on-line service provider, and member data refers to a connection telephone number to an on-line service.

[0023] In a case where the registered address or domicile of an on-line service member is used as member data, when a user establishes communication using a mobile computer in a place other than his home, the user is determined to be an unauthorized member user. Also, every time a user changes his address, the user is required to report the address change. In view of the above, the telephone number for connecting to an access point is used as member data (connection point data D1). This is because an on-line service member usually connects to an access point, a connection to which takes the cheapest telephone fee for an on-line service.

(Claim 3) The invention claimed in Claim 3, which is a technically limited version of the invention claimed in Claim 2, is characterized in that connection point data (D1) is entered by a on-line service member when connecting to on-line services.

[0024] When an on-line service member establishes communication using a mobile computer, connection point data may not be the address or the domicile of the on-line service member. In the invention claimed in Claim 3, connection point data is not obtained as in the case of the invention claimed in Claim2, but entered directly by a member user. This is because a user may select in view of communication speed an access point, a connection to which does not take the cheapest telephone fee.

(Claim 4) The invention claimed in Claim 4, which is a technically limited version of Claim 1, 2, or 3, is characterized in that an output for preventing a user from receiving an on-line services , which is produced when area data does not match member data, is an output for putting an on-line service member at a disadvantage.

(Definitions of Terms) The "output produced when area data does not match member data" refers to not only a "passive" output which terminates communication, but also an output which aggressively impairs the interests of a PC user such as software for freezing a computer used for communication or for displaying a warning screen.

[0025] In the invention according to Claim 4, the following operations are performed. When processing means determines that connection point data (D1) does not match area data (D2), in the personal authentication system of the present system, it is determined that a user who has started communication with a service provider (AA) is not an authorized member user. As a result, the user is put at a disadvantage by outputting means. By announcing the possibility of suffering a disadvantage, unauthorized users can be precluded.

(Claim 5) An invention claimed in Claim 5 is a personal authentication method for authenticating a user, when the user accesses a computer owned by a service provider (AA) providing services using information and communication technology, the personal authentication method comprising: a member data reading process for reading member data; a member data storing process for storing member data; a area data obtaining process for obtaining from a PHS carrier (PP) area data (D2) of a PHS terminal device (20) owned by a member user; a processing process for determining whether area data (D2) matches member data; and an output process, when as a result of a determination of the processing means area data matches member data, for producing an output for allowing a user to continue to receive services from a service provider (AA), and when area data does not match member data, for producing an output for preventing a user from receiving services from a service provider (AA).

(Claim 6) An invention claimed in Claim 6 is a personal authentication system comprising: connection point data reading means for reading connection point data (D1) via communication to a card company (CC) with a card (17) of a credit card member; contract data storing means for

pre-storing connection point data (D1) and card contract data; area data obtaining means for reading area data (D2) on the basis of an output from a PHS base station available for a PHS terminal device (20) owned by a credit card member; area service data storing means for storing area service data corresponding to area data (D2); and area service data outputting means for outputting area service data.
(Definitions of Terms) The "communication to a card company (CC) with a card (17) of a credit card member" refers to communication for checking the expiration date, etc. using a card reader (18) and a communication line such as a telephone (14) or a dedicated line.
[0026] The "are service data (D3)" is information which relates to the area where a PHS base station (P1) is located, and is useful for users of PHS terminal devices (20). Specifically, "area service data (D3)" includes simple and a small amount of data which can be output by a display or a speaker of a PHS terminal device (20) such as the name of the nearest station or the telephone number of the nearest access point, and a large amount of data which is output to a mobile computer connected with a PHS terminal device (20) such as a map of the area or an area shopping guide. Since "area service data (D3)" is data only for checking whether a user of a credit card is an authorized credit card member, the data is usually a small amount of data. Also, since "area service data D3" is provided to users who have completed all purchases, information is useful for the users such as the name of the nearest station, the last train time of the station, information on events of adjacent shops where the credit card can be used.
[0027] Area service data (D3) may be output to a PHS terminal device (20) owned by a card member as shown in Fig. 6, or output to a device owned by a shop (C1) which has a contract with a credit card company (CC) as shown in Fig. 8. The telephone number of a PHS terminal device (20) may be transmitted via a card reader (18) and a telephone (14) when conducting "communication to a card company (CC) with a card (17) of a credit card member". In such a case, if a card user is not an authorized card member, the user is expected to hesitate to tell a clerk of a shop of the telephone number of a PHS terminal device (20).
[0028] The operations of the invention according to Claim 6 will be described below. In the personal authentication system of the present invention, when communication to a credit card company (CC) is started with a card (17) of a credit card member, connection point data (D1) is read by connection point data reading means. The credit card company (CC) reads with area data reading means area data (D2) of a PHS terminal device (20) owned by the credit card member from a base station (for example, P1) nearest the PHS terminal device (20). The credit card company (CC) outputs area service data (D3) corresponding to the area data (D2) from area service data storing means.
[0029] When the card user is an authorized credit card member, the user receives the area service data (D3). Consequently, the shop can determine the card user to be an authorized credit card member, and makes a bargain with the user. When the card user is not an authorized credit card member, the shop can determine the card user not to be an authorized credit card member on the basis of the fact that the user can not receive the area service data (D3). This is because the user is very likely to be one who has obtained the credit card (17) illegally.
[0030] As in the invention claimed in Claim 1, to enable the personal authentication of the present invention, all a member user has to do is to have his/her PHS terminal device 20 at hand. This does not become a burden a member user because a user of a PHS terminal device (20) usually has his/her PHS terminal device (20) at hand.
(Claim 7) The invention claimed in Claim 7, which is a technically limited version of the invention claimed in Claim 6, is characterized by comprising determining means which, when area service data (D3) is output, determines that a credit card member is allowed to make a bargain by card, and when area service data (D3) is not output, determines that a credit card member is not allowed to make a bargain by card.
[0031] In short, In Claim 7, "determining means" has been added to the constituent features of Claim 6. In the invention claimed in Claim 6, since a determination by "determining means" may be performed by a clerk of a shop, "determining means" is not an indispensable constituent feature of Claim 6.

(Claim 8) An invention claimed in Claim 8 is a personal authentication method comprising: card contract data reading process for reading connection point data (D1) and card contract data via communication to a card company (CC) with a card (17) of a credit card member; area data obtaining process for reading area data (D2) on the basis of an output from a PHS base station available for a PHS terminal device (20) owned by a credit card member; area service data outputting process for outputting area service data (D3) corresponding to area data (D2); and determining process in which, when area service data (D3) is output, it is determined that a credit card member is allowed to make a bargain by card, and when area service data (D3) is not output, it is determined that a credit card member is not allowed to make a bargain by card.
(Claim 9) An invention claimed in Claim 9 is a personal authentication system for authenticating a user, when the user accesses a computer owned by a service provider providing services using information and communication technology, the personal authentication system comprising: connection point data obtaining means for obtaining connection point data of a member user; telephone number storing means for pre-storing communication terminals owned by member users and telephone numbers of the communication terminals; and authentication call means for reading a telephone number stored in the telephone number storing means and calling a communication terminal.
[0032] The "communication terminal" refers to a PHS phone, a beeper, and a common mobile phone.
(Claim 10) An invention claimed in Claim 10 is a personal authentication method for authenticating a user, when the user accesses a computer owned by a service provider providing services using information and communication technology, the personal authentication method comprising: telephone number storing process for pre-storing communication terminals owned by member users and telephone numbers of the communication terminals; connection point data obtaining process for obtaining connection point data of a member user; and authentication call process for reading a telephone number stored in telephone number storing means and calling a communication terminal.
[0033]
[Embodiments of the invention] The present invention will be explained below with reference to embodiments and Figs. 1-10. Fig. 1 is a conceptual diagram of the first embodiment of the present invention. Fig. 2 is a flowchart of the first embodiment of the present invention. Fig. 3 is a conceptual diagram of the second embodiment of the present invention. Fig. 4 is a conceptual diagram of the third embodiment of the present invention. Fig. 5 is a conceptual diagram of the fourth embodiment of the present invention. Fig. 6 is a conceptual diagram of the fifth embodiment of the present invention. Fig. 7 is a flowchart of the fifth embodiment of the present invention. Fig. 8 is a conceptual diagram of the sixth embodiment of the present invention. Fig. 9 is a conceptual diagram of the seventh embodiment of the present invention. Fig. 10 is a flowchart of the seventh embodiment of the present invention.
(The first embodiment) The first embodiment of the present invention will be explained with reference to Figs. 1 and 2. This first embodiment relates to a personal authentication system and method for authenticating a user when the user accesses a computer owned by on-line service provider AA providing services using information and communication technology.
[0034] To receive services provided by on-line service provider AA, a user is required to register the name, the address or the domicile, and a telephone number with on-line service provider AA. When a user completes the registration, the user become a member user. On-line service provider AA records in database (DB) member data (for example, the address or the domicile of a member). To receive services provided by on-line service provider AA, a member user establishes communication using hardware such as personal computer 12, modem 13, and telephone 14; communication software; a password arranged between the member user and on-line service provider AA; etc. When establishing communication, an appropriate access point is selected among access points A1, A2, A3, ... provided by on-line service provider AA in view of the distance, transmission speed, etc.

[0035] In this system, since a member user is assumed to own PHS terminal device 20, on-line service provider AA registers and records the telephone number or the identification number of PHS terminal device 20 as member data. PHS carrier (PP) locates a plurality of base stations P1, P2, P3, ... in the area, and each of base stations P1, P2, and P3 transmits via radio waves to PHS terminal device 20 information indicating a base station to be used in view of the current location of PHS terminal device 20. Therefore, for each PHS terminal device 20, the closest base station can be identified.

[0036] When a user starts to use an on-line service, on-line service provider AA reads member data of the user using the member data reading means. In this embodiment, on-line service provider AA, on the basis of the password, etc. of the user, accesses member data recorded in database (DB) to read the address or the domicile of the user.

[0037] Also, on-line service provider AA obtains from PHS carrier (PP) area data D2 which is information on a location of PHS terminal device 20 owned by the user. If both of base stations P1 and P2 are closer to PHS terminal device 20, correcting means provided in PHS carrier (PP) or on-line service provider AA selects either of radio waves Q1 and Q2 as area data D2.

[0038] On-line service provider AA is provided with processing means for determining whether member data matches area data D2. On-line service provider AA determines with the processing means whether member data matches area data D2. As a result of the determination, when member data matches area data D2, on-line service provider AA produces an output for allowing a user to continue to receive services from on-line service provider AA. When member data does not match area data D2, on-line service provider AA produces an output for preventing a user from receiving services from on-line service provider AA. In this embodiment, on-line service provider AA produces an output for unilaterally terminating the receipt of an on-line service.

[0039] When the user has PHS terminal device 20 at hand, the processing means determines that the member data matches area data D2. In such a case, the personal authentication system according to the present embodiment determines the user to be an authorized member user, and the user is allowed to continue to receive the on-line service by the outputting means.

[0040] On the other hand, a determination by the processing means that the member data does not match area data D2 indicates that the user does not have PHS terminal device 20 owned by an authorized member user at hand. Since it is unlikely that a user does not have his/her PHS terminal device 20 at hand, the access by the user is very likely to be an unauthorized one.

(The second embodiment) The second embodiment will be explained with reference to Fig. 3.

[0041] In the first embodiment, on-line service provider AA accesses member data on the basis of the password, etc. of a user to read the address or the domicile of the user. Consequently, when a user goes out with PHS terminal device 20 and establishes communication using a mobile computer in a place other than the address or the domicile, it is determined that the member data of the user does not match area data D2. Therefore, in the second embodiment, instead of addresses or domiciles recorded in a database, the telephone number of access point A1 (connection point data D1) is read as member data. Consequently, if a user goes out with a communications device and establishes communication in a place other than the address or the domicile, this personal authentication system works effectively.

[0042] Connection point data D1 may be input directly by a member. This is because a member may select in view of transmission speed an access point, a connection to which does not take the cheapest telephone fee.

(The third embodiment) The third embodiment will be explained with reference to Fig. 4.

[0043] In the third embodiment, a personal authentication system of the present invention is applied to transactions by cash card 15 issued by a bank. "Member data" refers to connection point data D1, namely the location of branch bank B1 where transactions by cash card 15 is performed. Fig. 4 shows that a user draws out cash from cash dispenser 16 with cash card 15.

[0044] When a user inserts cash card 15 into cash dispenser 16 and enters his/her personal identification code, cash dispenser 16 sends connection point data D1 to computer center BB. Computer center BB obtains from PHS carrier (PP) area data D2 of PHS terminal device 20 of an owner of cash card 15, and determines whether connection point data D1 matches area data D2.

When it is determined that connection point data D1 matches area data D2, computer center BB produces an output for allowing the user to draw out cash. When it is determined that connection point data D1 does not match area data D2, computer center BB produces an output to cash dispenser 16 for preventing the user from drawing out cash.

(The fourth embodiment) The fourth embodiment will be explained with reference to Fig. 5.

[0045] In the fourth embodiment, a personal authentication system of the present invention is applied to transactions by credit card 17 issued by credit card company CC. "Member data" refers to connection point data D1, namely the location of shop C1 which has a card use contract for making credit card 17 usable in shop C1. Fig. 5 shows that when a user purchases goods by credit card 17, card reader 18 inquiring for the expiration date, etc. of credit card 17 reads credit card 17.

[0046] Card reader 18, when reading magnetically recorded information of credit card 17, sends the information to credit card company CC via telephone 14 (or a dedicated line). Credit card company CC reads card use contract data. Also, credit card company CC obtains from PHS carrier (PP) area data D2 of PHS terminal device 20 of an owner of credit card 17, and determines whether connection point data D1 matches area data D2. When it is determined that connection point data D1 matches area data D2, credit card company CC produces an output for allowing the user to use credit card 17. When it is determined that connection point data D1 does not match area data D2, credit card company CC produces an output to card reader 18 for preventing the user from using credit card 17.

(The fifth embodiment) The fifth embodiment will be explained with reference to Figs. 6 and 7. In the fifth embodiment, a personal authentication system of the present invention is applied to transactions by credit card 17 issued by credit card company CC, and the fifth embodiment is a modification of the fourth embodiment.

[0047] The fifth embodiment differs from the fourth embodiment in having a system where service data is output to PHS terminal device 20 which should be possessed by a user of credit card 17. In the fifth embodiment, there exist area service data storing means for storing area service data corresponding to area data D2 and area service data outputting means for outputting area service data D3 to PHS terminal device 20 of a credit card member.

[0048] In the fifth embodiment, card reader 18 is provided with determining means 19 for connecting to PHS terminal device 20 and determining whether area service data D3 has been output to PHS terminal device 20. "Area service data D3" is information which relates to the area where PHS base station P1 is located, and is useful for a user of PHS terminal device 20. Specifically, "area service data D3" is the name of the nearest station, the last train time of the station, information on events of adjacent shops where credit card 17 can be used, since it is provided to users who has completed all purchases.

[0049] In the present embodiment, when a card user is an authorized credit card member, the user receives area service data D3 with PHS terminal device 20 at hand. When the receipt is recognized by determining means 19, shop C1 can determine the card user to be an authorized credit card member, and makes a bargain with the user. If the user is not an authorized credit card member, determining means 19 is to determine that the user can not receive area service data D3 with PHS terminal device 20 at hand. On the basis of the determination, shop C1 can determine the card user not to be an authorized credit card member. This is because the user is very likely to be one who has obtained credit card 17 illegally.

(The sixth embodiment) The sixth embodiment will be explained with reference to Fig. 8.

[0050] In the sixth embodiment, a personal authentication system of the present invention is applied to transactions by credit card 17 issued by credit card company CC, and the sixth embodiment is a modification of the fifth embodiment. The sixth embodiment differs from the fifth embodiment in that area service data D3 is output to speaker 19 connected to a device of shop C1 such as card reader 18. When area service data D3 is not output or does not relate to the area where shop C1 is located, a transaction by credit card 17 is suspended.

[0051] In the above-mentioned first to sixth embodiments, all a user has to do for personal authentication is to have PHS terminal device 20 at hand. A user is never required to remember a new personal identification code or to carry a new key with the user.
(The seventh embodiment) The seventh embodiment will be explained with reference to Figs. 9 and 10.
[0052] In the seventh embodiment, a personal authentication system of the present invention is applied to transactions by credit card 17 issued by credit card company CC. Also, in this personal authentication system which has a simplified configuration, not only PHS terminal devices but also beepers or common mobile phones can be used. In the seventh embodiment, telephone numbers of PHS terminal devices 20 of member users are pre-recorded in a database. When a user purchases goods by credit card 17, information recorded in credit card 17 is read by card reader 18, connection point data D1 is sent to credit card company CC via a communication line of shop C1 such as telephone 14. Credit card company CC, when obtaining connection point data D1, reads the telephone number of the user recorded in the database, and calls PHS terminal device 20 for authenticating the user.
[0053] When PHS terminal device 20 of the user receives a call for authentication from credit card company CC, a clerk of shop C1 presumes on the basis of the call reception the user to be an authorized member and accepts the transaction by credit card 17. When a call for authentication is not received, a clerk of shop C1 presumes the user not to be an authorized member and tells the user that the transaction by credit card 17 cannot be accepted.
[0054] PHS terminal device 20, which is used as a mobile communication terminal in the seventh embodiment, may be a beeper or a common mobile phone. In the seventh embodiment, all a user has to do for personal authentication is to have PHS terminal device 20 at hand. A user is never required to remember a new personal identification code or to carry a new key with the user.
[0055]
[Effects of the Invention] According to the inventions claimed in Claims 1 to 3, and Claim 9, a personal authentication system is provided which does not excessively complicate authentication information held by authenticated member users and does not force on member users too many operations than before. According to the invention claimed in Claim 4, a personal authentication system is provided which makes it possible to preclude unauthorized users by putting them at a disadvantage.
[0056] According to the inventions claimed in Claims 5 and 10, a personal authentication method is provided which does not excessively complicate authentication information held by authenticated member users and does not force on member users too many operations than before. According to the inventions claimed in Claims 6 and 7, a personal authentication system is provided which does not excessively complicate authentication information held by authenticated credit card members and does not force on card members too many operations than before.
[0057] According to the invention claimed in Claim 8, a personal authentication method is provided which does not excessively complicate authentication information held by authenticated credit card members and does not force on card members too many operations than before.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－198636

(43)公開日　平成10年(1998)７月31日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ
	17/60		Ｈ０４Ｍ	11/08	
Ｈ０４Ｌ	9/32			3/42	Ｚ
Ｈ０４Ｍ	11/08		Ｇ０６Ｆ	15/21	３４０Ｂ
// Ｈ０４Ｑ	7/38		Ｈ０４Ｌ	9/00	６７１

審査請求　未請求　請求項の数10　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願平9－3420

(22)出願日　平成９年(1997)１月13日

(71)出願人　000155469
株式会社野村総合研究所
東京都中央区日本橋１丁目10番１号

(72)発明者　藤元　健太郎
横浜市保土ヶ谷区神戸町134番地　株式会社野村総合研究所内

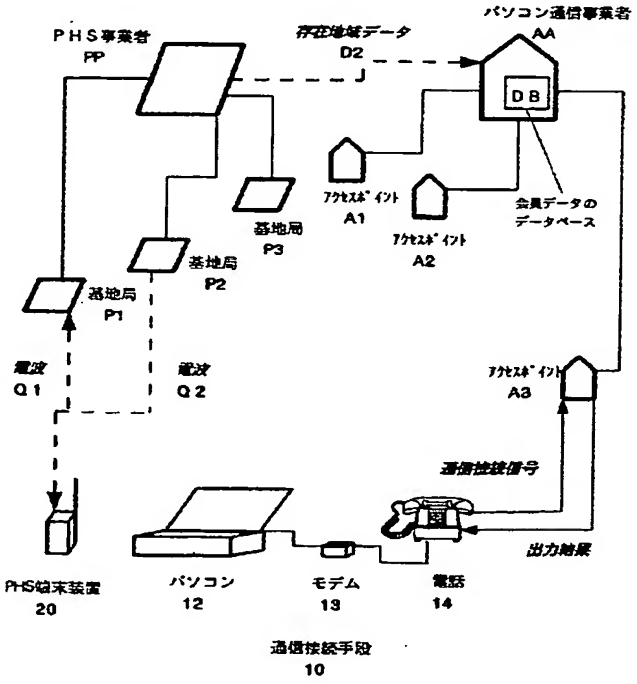
(74)代理人　弁理士　黒田　博道　（外４名）

(54)【発明の名称】　個人認証システムおよび個人認証方法

(57)【要約】

【目的】　正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない認証技術を提供する。

【構成】　会員ユーザに関する会員データ（例えば、会員の住所または居所）を読み込む会員データ読込手段、会員ユーザが所有するＰＨＳ端末装置(20)の存在地域データ(D2)をＰＨＳ事業者(PP)から取得する存在地域データ取得手段、会員データと存在地域データ(D2)との一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力手段を備える。



1

【特許請求の範囲】

【請求項１】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザに関する会員データを記憶する会員データ記憶手段、会員データを読み込む会員データ読込手段、会員ユーザが所有するＰＨＳ端末装置の存在地域データをＰＨＳ事業者から取得する存在地域データ取得手段、会員データと存在地域データとの一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者からの利益享受を継続できるとともに、不一致の場合にはサービス提供者からの利益を取得できないような出力結果を出力する出力手段を備えたことを特徴とする個人認証システム。

【請求項２】サービス提供者をパソコン通信事業者とし、

会員データは、パソコン通信の接続電話番号によって認識することとしたことを特徴とする請求項１記載の個人認証システム。

【請求項３】会員データは、パソコン通信会員がパソコン通信の接続時に入力することとしたことを特徴とする請求項２記載の個人認証システム。

【請求項４】演算の結果が不一致の場合にパソコン通信による利益を取得できないような出力結果は、そのパソコン通信会員に不利益をもたらすための出力結果としたことを特徴とする請求項１、請求項２または請求項３の個人認証システム。

【請求項５】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザに関する会員データを読み込む会員データ読込工程、会員ユーザに関する会員データを記憶する会員データ記憶工程、会員ユーザが所有するＰＨＳ端末装置の存在地域データをＰＨＳ事業者から取得する存在地域データ取得工程、会員データと存在地域データとの一致判断を行う演算工程、および演算手段の判断の結果、一致している場合にはサービス提供者からの利益享受を継続できるとともに、不一致の場合にはサービス提供者からの利益を取得できないような出力結果を出力する出力工程を含むことを特徴とする個人認証方法。

【請求項６】クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データを読み込む接続地域データ読込手段、予め接続地域データを記憶している接続地域データ記憶手段、クレジットカード会員が所有するＰＨＳ端末装置の存在地域データをＰＨＳ事業者から取得する存在地域データ取得手段、存在

2

地域データに対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータの内容を出力する地域サービスデータ出力手段を備えたことを特徴とする個人認証システム。

【請求項７】地域サービスデータの出力があった場合にはクレジット会員が取引契約を締結できると判断するとともに、地域サービスデータの出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断手段を備えたことを特徴とする請求項６記載の個人認証システム。

【請求項８】クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データおよびカード契約データを読み込むカード契約データ読込工程、クレジットカード会員が所有するＰＨＳ端末装置の存在地域データをＰＨＳ事業者から取得する存在地域データ読込工程、存在地域データに対応する地域サービスデータの内容を出力する地域サービスデータ出力工程、および地域サービスデータの出力があった場合にはクレジット会員がカード契約を締結できると判断するとともに、地域サービスデータの出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断工程を含むことを特徴とする個人認証方法。

【請求項９】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザの接続地域データを取得する接続地域データ取得手段、会員ユーザが所有する通信端末装置、その通信端末装置の電話番号を予め記憶している電話番号記憶手段、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール手段を備えたことを特徴とする個人認証システム。

【請求項１０】情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザが所有する通信端末装置の電話番号を予め記憶している電話番号記憶工程、会員ユーザの接続地域データを取得する接続地域データ取得工程、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール工程を備えたことを特徴とする個人認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、個人認証システムおよび個人認証方法、更に詳しくは、パソコン通信やクレジットカード等の電子的手段を用いて行う物品購入等の契約において、本人認証をより確実にするためのシステムおよびその方法に関する。

3

【０００２】

【先行技術】従来より、電子的手段を用いての契約、取引などが行われるに際し、その電子的手段を用いている者が正規の契約者であるか否かの認証は、暗証番号、パスワードなどによって行われてきた。例えば、パソコン通信（いわゆるインターネット通信でも同じ）であれば、パソコンおよび電話回線を用いてパソコン通信の会員が申込情報を送信し、事業者側に設置されたコンピュータシステムではこれを受信することで、その両者間の契約を行ってきた。この際、そのパソコン通信会員が正規の契約手順を踏んでいるか否かを認証するため、従来から行われてきている基本的手段は次のようなものである。

【０００３】まず、予めパソコンユーザとパソコン通信事業者との間で利用契約を締結する。その際、事業者が正規会員ユーザへ会員ＩＤ番号、パスワードを決定して知らせる。事業者は、パソコン通信を介してユーザからアクセス要求があったときには、アクセス者に対して予め登録させた会員ＩＤおよびパスワードを要求し、アクセス者がこれを入力したときに事業者側に記録されている正規会員情報と照合して、これに適合したときには、アクセス者を正規の会員ユーザと認定する。そして、その通信接続中に送信されてくる注文情報等は、その正規の会員ユーザが送信したものと擬制してこれを受け付けるというものである。

【０００４】更に、この正規契約者による正規契約手順が踏まれているか否かの確認をより厳格にするために、事業者側から会員ＩＤ番号とパスワードが要求されたときにユーザが入力できる時間を制限したり、誤った入力を一定回数以上行った場合にはこれを不正なアクセス者であると判断して回線を切断する、などの手段によって不正なアクセス者を排除しようとしている。

【０００５】

【発明が解決しようとする課題】しかしながら、不正なアクセス者を排除せんとする上記のような方法は、例えばハッカー（不正侵入者）が正規会員ユーザのパソコンの送信ゲートなりモデムなりに侵入し、ここで正規会員ユーザが送信する会員ＩＤ番号やパスワードを取得してしまえば、無力化する。予め設定された会員ＩＤ番号およびパスワードも何らかの手段で他者が知った場合は、本人認証としてはその役目を果たさなくなる。

【０００６】一方、ハッカーによる会員ＩＤ番号およびパスワードの不正取得を防止することを目的に、正規会員ユーザと事業者間では情報の伝達を暗号処理し、通信セキュリティを確保して行われることがある。しかし、パスワード等の不正取得を防止する手段を如何に高度化、複雑化させたところで、より高度な不正取得手段を開発するハッカーとの間では何ら本質的な解決策とはならない。

【０００７】この類の事件は、従来から銀行カードやクレジットカードにおいても発生している。特に正規会員ユーザが設定するパスワードは、その忘失を恐れて自己ないしは近親者の誕生日や電話番号の下四桁を活用することも少なくないため、これを悪用しようとする者からすれば比較的容易にパスワードを察知することができ、結果として不正に財貨を取得することができる。

4

【０００８】本発明が解決すべき課題は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない認証技術を提供することにある。ここで、請求項１ないし請求項３および請求項９記載の発明の目的は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証システムを提供することである。

【０００９】請求項４記載の発明の目的は、更に、不正なアクセス者に不利益を被らせるようなシステムとすることによって、結果的に不正なアクセス者を未然防止できる個人認証システムを提供することである。請求項５および請求項１０記載の発明は、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証方法を提供することである。

【００１０】請求項６および請求項７記載の発明の目的は、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証システムを提供することである。請求項８記載の発明の目的は、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証方法を提供することである。

【００１１】

【課題を解決するための手段】上記した課題を解決するため、本出願人は、前記した請求項１ないし請求項１０に記載した発明を提供する。本願に係る発明は、昨今急速に普及しているＰＨＳ端末装置、ポケットベル、携帯電話をシステムの正規の会員ユーザが所有していること、且つそのＰＨＳ端末装置が常にその正規の会員ユーザの手元に存在していることを前提としている。請求項１ないし請求項８では、ＰＨＳ端末装置の位置情報を入手しているＰＨＳ通信事業者からその位置情報を取得し、電子的手段を用いての契約、取引など行おうとしている者がどこにいるかを確認し、通信接続地とＰＨＳ端末装置の位置情報とが異なる場合には、これを不正と判断するのである。

【００１２】請求項９および請求項１０では、ＰＨＳ端末装置に限られず、ポケットベル、通常の携帯電話の場合も含め、取引直後のコールの有無で不正を判断するのである。

（請求項１）請求項１記載の発明は、情報通信を用いてサービスを提供するサービス提供者（例えば、パソコン

5

通信事業者AA）が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザに関する会員データを記憶する会員データ記憶手段、会員ユーザに関する会員データ（例えば、会員の住所または居所）を読み込む会員データ読込手段、会員ユーザが所有するＰＨＳ端末装置(20)の存在地域データ(D2)をＰＨＳ事業者(PP)から取得する存在地域データ取得手段、会員データと存在地域データ(D2)との一致判断を行う演算手段、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力手段を備えたことを特徴とする。

（用語定義）「会員ユーザ」とは、本発明に係る個人認証システムを利用できる正規の会員であり、本システムを運用するサービス提供者（例えば、パソコン通信事業者(AA)、キャッシュカードを発行する銀行(BB)、クレジットカード会社(CC)など）への登録を済ませた者をいう。クレジットカードが買い物をする際に使用できるようにクレジットカード会社(CC)との契約を済ませた商店（C1）は、ここにいう「会員ユーザ」には含まない。

【００１３】会員ユーザがサービス提供者のサービスを受けるには、通信接続手段(10)が必要である。通信接続手段(10)とは、例えばサービス提供者との通信の接続に必要不可欠な「通信接続信号」を発信する手段のことをいう。本システムがパソコン通信において採用されている場合には、パソコン(12)およびモデム(13)というハードウエアと通信ソフトウエアやパスワードなどのソフトウエアなどをいう。また、本システムがキャッシュカード(15)やクレジットカード(17)による取引において採用されている場合には、カード本体(15,17)とそのカード本体(15,17)に記録されたデータや暗証番号などのソフトウエアなどをいう。銀行のキャッシュカード(15)が使用できるキャッシュディスペンサー(16)やクレジット会社(CC)との契約を済ませた商店(C1)に設置されたカードリーダー(18)は、ここにいう「通信接続手段(10)」の一部を構成する。

【００１４】「会員データ」とは、例えば会員ユーザの住所または居所、電話番号など、予めサービス提供者がそのデータベースに蓄えているデータである。「会員データ記憶手段」とは、予めデータを記憶している記憶装置の他、通信接続時に読み込んだデータを記憶する装置も含む場合もある。本発明の個人認証システムがパソコン通信において採用されている場合には、会員ユーザに属する通信接続手段(10)（例えば、パソコン12、モデム13などのパソコン通信機器）を用いてサービス提供者への通信を開始したときの接続地域データ(D1)を「会員データ」とすることができる。更に、その「接続地域データ(D1)」は、通常はパソコン通信会員の住所または居所であるので、パソコン通信事業者(AA)に登録されており、その会員データのデータベースに蓄積されている。また、この接続地域データ(D1)を、その接続地域のデータとして接続時に読み込むものとすれば、パソコン通信機器を会員ユーザの住所または居所以外の場所に持ち出して接続しても、本発明の個人認証システムは機能することとなる。

【００１５】なお、本システムがキャッシュカード(15)やクレジットカード(17)による取引において採用されている場合には、会員データは「接続地域データ(D1)」となり、キャッシュカード(15)やクレジットカード(17)によって取引契約を使用とする支店や店の所在地などとなる。その場合、会員データたる「接続地域データ(D1)」は銀行が管理するコンピュータセンター(BB)やカード会社(CC)に登録されてデータベースに蓄積されているとともに、銀行支店や商店(C2)に設置されたキャッシュディスペンサー(16)やカードリーダー(18)からコンピュータセンター(BB)やカード会社(CC)へ発信される。

【００１６】「存在地域データ(D2)」とは、通信時にＰＨＳ端末装置(20)が使用することができるＰＨＳ基地局(例えばP1)の所在地のことであり、ＰＨＳ基地局(例えばP1)が受信したものを使用する。通常は、ＰＨＳ端末装置(20)とＰＨＳ基地局(P1)とは、絶えず定期的に基地局ＩＤを電波にて送受信している。本システムを運用するサービス提供者(AA)は、この基地局ＩＤにて認識できる存在地域データ(D2)を、ＰＨＳ基地局(P1)を介してＰＨＳ事業者(PP)から取得する。

【００１７】本システムがパソコン通信において採用されている場合であって、図３に示すように会員ユーザが当該ＰＨＳ端末装置(20)をパソコン(12)のモデム(13)に接続してパソコン通信を行った場合、「存在地域データ」は、その通信を接続したＰＨＳ基地局(P3)の所在地とすることができる。「演算手段」とは、例えば「会員データ」と「存在地域データ」が単純なデータである場合には、両データの解読とテーブルによる対応とを行う装置をも含む趣旨である。例えば、図１に示すように複数のＰＨＳ基地局(P1,P2)による存在地域データ(D2)が読み込まれる可能性がある場合には、「会員データと存在地域データとの一致判断」は、補正手段などによって一致していると判断する。

【００１８】「不一致の場合の出力結果」とは、通常は、通信または取引を継続することができないように回線を接続することであるが、通信を継続することによって不利益をもたらされるような出力であってもよい。例えば、クレジットカードを無効とするためにカードの記録データを書き換えるためのデータ出力などが該当する。なおこれに付属して、正規の会員に対して、不正に使用されているおそれがある旨を、信用機関等を通じて連絡することとしてもよい。

7

【００１９】請求項１記載の発明に係る個人認証システムによれば、以下のような作用をなす。まず、会員ユーザがサービス提供者(AA)への通信を開始し、本発明に係る個人認証システムは会員データ読込手段にて会員データを読み込む。また、サービス提供者(AA)は、会員ユーザが所有するＰＨＳ端末装置(20)の存在地域データ(D2)を、存在地域データ取得手段にてＰＨＳ事業者(PP)から出力によって読み込む。そして、記憶手段によって予め記憶している会員データと存在地域データ(D2)との一致判断を、演算手段によって行う。

【００２０】このとき、会員ユーザは自分が所有するＰＨＳ端末装置(20)を手元に置いてあるとすると、演算手段は会員データと存在地域データ(D2)とが一致していると判断する。その場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザであると判断し、出力手段によって会員ユーザはサービス提供者(AA)からの利益享受を継続できる。

【００２１】一方、その演算手段が会員データと存在地域データ(D2)とが一致していないと判断した場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザでないと判断する。すると、出力手段によってその通信を開始した者は、サービス提供者(AA)からの利益を取得できない。サービス提供者(AA)への通信を開始した者の手元に、正規の会員ユーザが所有するＰＨＳ端末装置(20)が存在しないこととなっており、不正なアクセスである可能性が極めて高いからである。

【００２２】以上のように、会員ユーザに対して本発明に係る個人認証システムが新たに強いる負担は、自分が所有するＰＨＳ端末装置(20)を手元に置いておくことのみである。これは、会員ユーザに対しての負担にはならない。携帯用通信端末機の性格上、自分が所有するＰＨＳ端末装置(20)を手元に置いておくことはあたりまえだからである。

（請求項２）請求項２記載の発明は請求項１記載の発明をパソコン通信の場合に限定したものであり、サービス提供者をパソコン通信事業者とし、会員データは、パソコン通信の接続電話番号によって認識することとしたことを特徴とする。

【００２３】会員データを、会員登録時のパソコン通信会員の住所または居所とすると、携帯用パソコンを用いて自宅以外の場所から通信すると正規の会員でないと判断されてしまう。また、転居をした場合には、その度に届け出をしなければならない。そこで、通信のアクセスポイントの接続電話番号を会員データ（接続地域データD1）として認識することとしたものである。パソコン通信会員は、パソコン通信に要する電話料金が最も安いアクセスポイントへ接続するのが一般的だからである。

（請求項３）請求項３記載の発明は、請求項２記載の発明を技術的に限定したものであり、接続地域データ(D1)

8

は、パソコン通信会員がパソコン通信の接続時に入力することとしたことを特徴とする。

【００２４】携帯用パソコンによって通信する場合、接続地域データがパソコン通信会員の住所または居所ではないことがありえる。その場合、請求項２のように接続地域データを決めることもできるが、会員に直接入力してもらうのが本請求項記載の発明である。通信速度の関係で、アクセスポイントを電話料金が最も安いものとしない場合があるからである。

（請求項４）請求項４記載の発明は、請求項１、請求項２または請求項３の発明を技術的に限定したものであり、演算の結果が不一致の場合にパソコン通信による利益を取得できないような出力結果は、そのパソコン通信会員に不利益をもたらすための出力結果としたことを特徴とする。

（用語定義）「不利益をもたらすため出力結果」とは、通信を継続できなかったり終了させてしまうという消極的な出力結果のほか、当該パソコンの使用者の利益を積極的に害するような出力のことである。例えば、通信に用いているパソコンをフリーズさせたり、当該パソコンに警告表示画面を表示させるためのソフトウエアなどである。

【００２５】請求項４記載の発明によれば、前記請求項記載の発明と異なり、以下のような作用をなす。すなわち、演算手段が接続地域データ(D1)と存在地域データ(D2)とが一致していないと判断した場合、本発明に係る個人認証システムは、サービス提供者(AA)への通信を開始した者が正規の会員ユーザでないと判断する。そして、その通信を開始した者は、出力手段によって不利益を被る。この不利益を被るおそれの告知により、結果として不正なアクセス者を未然防止することができる。

（請求項５）請求項５記載の発明は、情報通信を用いてサービスを提供するサービス提供者(AA)が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザに関する会員データを読み込む会員データ読込工程、会員ユーザに関する会員データを記憶する会員データ記憶工程、会員ユーザが所有するＰＨＳ端末装置(20)の存在地域データ(D2)をＰＨＳ事業者(PP)から取得する存在地域データ取得工程、会員データと存在地域データ(D2)との一致判断を行う演算工程、および演算手段の判断の結果、一致している場合にはサービス提供者(AA)からの利益享受を継続できるとともに、不一致の場合にはサービス提供者(AA)からの利益を取得できないような出力結果を出力する出力工程を含むことを特徴とする。

（請求項６）請求項６記載の発明は、クレジットカード会員のカード(17)を用いてカード会社(CC)への通信することによって接続地域データ(D1)を読み込む接続地域デ

9

ータ読込手段、予め接続地域データ(D1)およびカード契約データを記憶している契約データ記憶手段、クレジットカード会員が所有するＰＨＳ端末装置(20)が使用可能な最寄りのＰＨＳ基地局からの出力によって存在地域データ(D2)を読み込む存在地域データ取得手段、存在地域データ(D2)に対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータ(D3)の内容を出力する地域サービスデータ出力手段を備えたことを特徴とする個人認証システムである。

（用語定義）「クレジットカード会員のカード(17)を用いてカード会社(CC)への通信する」とは、カードリーダー(18)および電話(14)または専用回線などの通信回線を用いて、かかるカード(17)の有効期限等のチェックを行うなどのための通信を行うことをいう。

【００２６】「地域サービスデータ(D3)」とは、ＰＨＳアンテナ基地局(P1)が位置する地域に関し、ＰＨＳ端末装置(20)のカード会員にとって有益な情報のことである。具体的には、最寄り駅名、最寄りのパソコン通信アクセスポイントの電話番号などＰＨＳ端末装置(20)の表示画面やスピーカーによって出力可能な簡単且つ短いデータや、携帯用パソコンなどに接続して取り出すような大きなデータ；例えば近傍の地図、地域ショッピングガイドなどである。ただし、クレジットカードを使用しようとした者が正規のクレジットカード会員か否かを確かめるための出力であるので、短い出力であることが多い。特に、買い物を済ませた会員に対しての情報であるので、最寄り駅名、その最寄り駅の終電車時刻、当該クレジットカードが使用できる最寄りの商店のイベント情報などが有益である。

【００２７】地域サービスデータ(D3)は、図６に示すように、カード会員の所有するＰＨＳ端末装置(20)をその出力装置としてもよいし、図８に示すように、クレジットカード会社(CC)との契約を済ませた商店（C1）が所有する機器に出力することとしてもよい。ＰＨＳ端末装置(20)の電話番号は、「クレジットカード会員のカード(17)を用いてカード会社(CC)への通信する」際に、カードリーダー(18)、電話(14)など機器を用いて送信することとしてもよい。その場合、カード使用者が正規のカード会員でない場合にはＰＨＳ端末装置(20)の電話番号を商店の店員に告げる際に躊躇することとなる。

【００２８】次に、請求項６記載の発明の作用を説明する。まず、クレジットカード会員のカード(17)を用いてカード会社(CC)への通信を開始し、本発明に係る個人認証システムは接続地域データ読込手段にて接続地域データ(D1)を読み込む。また、カード会社(CC)は、クレジットカード会員が所有するＰＨＳ端末装置(20)の存在地域データ(D2)を、存在地域データ取得手段にて最寄りの基地局(例えばP1)から出力によって読み込む。そして、存在地域データ(D2)に対応する地域サービスデータ(D3)を地域サービスデータ記憶手段から出力する。

10

【００２９】このとき、カード使用者が正規のクレジットカード会員であるとすると、地域サービスデータ(D3)を受け取ることとなり、商店側はそのカード使用者が正規のクレジットカード会員であると判断できる。その後、取引契約を締結すればよい。一方、カード使用者が正規のクレジットカード会員でないとすると、地域サービスデータ(D3)を受け取れないことを理由として、商店側はそのカード使用者が正規のクレジットカード会員でないと判断できる。クレジットカード(17)のみを不正に取得した者がそのカード(17)を使用している可能性が極めて高いからである。

【００３０】請求項１記載の発明と同じように、会員ユーザに対して本発明に係る個人認証システムが新たに強いる負担は、自分が所有するＰＨＳ端末装置(20)を手元に置いておくことのみである。これは、会員ユーザに対しての負担にはならない。携帯用通信端末機の性格上、自分が所有するＰＨＳ端末装置(20)は手元にあるのが普通だからである。

（請求項７）請求項７記載の発明は、請求項６記載の発明を技術的に限定したものであり、地域サービスデータ(D3)の出力があった場合にはクレジット会員が取引契約を締結できると判断するとともに、地域サービスデータ(D3)の出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断手段を備えたことを特徴とする。

【００３１】すなわち、請求項６の構成要件に「判断手段」を加えたものである。換言すると、請求項６記載の発明において「判断手段」を必須構成要件としていないのは、かかる判断を人為手段、すなわち商店の店員が行うこととする場合があるからである。

（請求項８）請求項８記載の発明は、クレジットカード会員のカードを用いてカード会社への通信することによって接続地域データ(D1)およびカード契約データを読み込むカード契約データ読込工程、クレジットカード会員が所有するＰＨＳ端末装置(20)が使用可能な最寄りのＰＨＳ基地局からの出力によって存在地域データ(D2)を読み込む存在地域データ読込工程、存在地域データ(D2)に対応する地域サービスデータ(D3)の内容を出力する地域サービスデータ出力工程、および地域サービスデータ(D3)の出力があった場合にはクレジット会員がカード契約を締結できると判断するとともに、地域サービスデータ(D3)の出力がない場合にはクレジット会員がカード契約を締結できないと判断する判断工程を含むことを特徴とする個人認証方法である。

（請求項９）請求項９記載の発明は、情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証システムであって、会員ユーザの接続地域データを取得する接続地域データ

取得手段、会員ユーザが所有する通信端末装置、その通信端末装置の電話番号を予め記憶している電話番号記憶手段、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール手段を備えたことを特徴とする。

【００３２】ここで、「通信端末装置」とは、ＰＨＳ、いわゆるポケットベルの他、通常の携帯電話をも含む趣旨である。

（請求項１０）情報通信を用いてサービスを提供するサービス提供者が保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合において、接続者が正規の会員ユーザであるか否かを認証する個人認証方法であって、会員ユーザが所有する通信端末装置の電話番号を予め記憶している電話番号記憶工程、会員ユーザの接続地域データを取得する接続地域データ取得工程、および電話番号記憶手段に記憶された電話番号を読み込んで通信端末装置へ電話をかける認証コール工程を備えたことを特徴とする。

【００３３】

【発明の実施の形態】以下、本発明を実施の形態および図面に基づいて更に詳しく説明する。ここで使用する図面は図１ないし図１０である。図１は、本発明の第一の実施の形態を示す概念図である。図２は、本発明の第一の実施の形態を示すフローチャートである。図３は、本発明の第二の実施の形態を示す概念図である。図４は、本発明の第三の実施の形態を示す概念図である。図５は、本発明の第四の実施の形態を示す概念図である。図６は、本発明の第五の実施の形態を示す概念図である。図７は、本発明の第五の実施の形態を示すフローチャートである。図８は、本発明の第六の実施の形態を示す概念図である。図９は、本発明の第七の実施の形態を示す概念図である。図１０は、本発明の第七の実施の形態を示すフローチャートである。

（第一の実施の形態）まず、図１および図２に基づいて、本発明の第一の実施の形態を説明する。この第一の実施の形態は、情報通信を用いてサービスを提供するパソコン通信事業者ＡＡが保有するコンピューターに、そのサービスの提供を受けようとする会員ユーザが接続する場合に採用されるシステムであって、接続者が正規の会員ユーザであるか否かを認証する個人認証システムおよび個人認証方法である。

【００３４】パソコン通信事業者ＡＡの提供するサービスを受けるためには、氏名、住所または居所、電話番号などをパソコン通信事業者ＡＡに登録し、この登録を済ませた者が会員ユーザとなる。パソコン通信事業者ＡＡは、そのデータベース（ＤＢ）に会員ユーザに関する会員データ（例えば、会員の住所または居所）を記録しておく。会員ユーザは、パソコン通信事業者ＡＡの提供するサービスを受けるため、パソコン１２、モデム１３および電話１４というハードウエアと通信ソフトウエアや、パソコン通信事業者ＡＡとの間で取り決められたパスワード等とを用いて、通信を接続する。接続は、パソコン通信事業者ＡＡが提供するアクセスポイントＡ１，Ａ２，Ａ３，・・・の中から、距離や通信速度などを勘案して適当なものを選んで行う。

【００３５】一方、本システムにおいては、会員ユーザがＰＨＳ端末装置２０を所有していることを前提としている。したがって通常、パソコン通信事業者ＡＡは、そのＰＨＳの電話番号や識別番号をも会員データとして登録、記憶している。ＰＨＳ事業者（ＰＰ）は、エリア内に多数の基地局Ｐ１，Ｐ２，Ｐ３，・・・を設置しており、それぞれの基地局Ｐ１，Ｐ２，Ｐ３からはＰＨＳ端末装置２０に対して、現在のＰＨＳ端末装置２０の位置によればどの基地局を使用するか、という情報を電波により発信している。したがって、どのＰＨＳ端末装置２０が、どの基地局の近傍に存在するかという存在地域の情報を取得できる。

【００３６】パソコン通信事業者ＡＡは、あるユーザがパソコン通信に接続を開始した場合、そのユーザに対応する会員データを会員データ読込手段によって読み込む。この実施の形態にあっては、接続があったユーザのパスワード等から、データベース（ＤＢ）に記憶された会員データにアクセスしてその住所または居所を読み込む。

【００３７】一方、その会員ユーザが所有するＰＨＳ端末装置２０の存在地域の情報たる存在地域データＤ２を、ＰＨＳ事業者（ＰＰ）から取得する。なお、最寄りの基地局としてＰ１，Ｐ２の二つがある場合、電波Ｑ１，Ｑ２のいずれを存在地域データＤ２とするかは、ＰＨＳ事業者（ＰＰ）またはパソコン通信事業者ＡＡに設けられた補正手段によって定められるものとする。

【００３８】パソコン通信事業者ＡＡは、会員データと存在地域データＤ２との一致判断を行う演算手段を備えており、その演算手段によって両データの一致を判断する。判断の結果、一致している場合にはパソコン通信事業者ＡＡからの利益享受を継続できるとともに、不一致の場合にはパソコン通信事業者ＡＡからの利益を取得できないような出力結果を出力する。この実施の形態にあっては、パソコン通信をパソコン通信事業者ＡＡ側から一方的に終了させるという出力をする。

【００３９】会員ユーザは自分が所有するＰＨＳ端末装置２０を手元に置いてあるとすると、演算手段は会員データと存在地域データＤ２とが一致していると判断する。その場合、本実施の形態に係る個人認証システムは、通信を開始した者が正規の会員ユーザであると判断し、出力手段によって会員ユーザはパソコン通信による利益享受を継続できる。

【００４０】一方、その演算手段が会員データと存在地域データ(D2)とが一致していないと判断した場合とは、通信を開始した者の手元に正規の会員ユーザが所有する

13

ＰＨＳ端末装置２０が存在しないということである。自分が所有するＰＨＳ端末装置２０が手元にないという事態は通常はあり得ないことであり、不正なアクセスである可能性が極めて高いからである。

（第二の実施の形態）続いて、図３に基づいて第二の実施の形態について説明する。

【００４１】第一の実施の形態にあっては、接続があったユーザのパスワード等から会員データにアクセスしてその住所または居所を読み込むこととしているので、ＰＨＳ端末装置２０を持って外出し、携帯用のパソコンによって住所または居所以外のところで通信を開始すると、会員データと存在地域データＤ２とが一致しないと判断されてしまう。そこで、第二の実施の形態にあっては、予めデータベースに記憶されている会員の住所または居所を会員データとしては用いず、アクセスポイントＡ１から接続したことを、その電話番号などと置き換え、その接続地域データＤ１を会員データとして読み込むこととする。この接続地域データＤ１を、その接続地域のデータとして接続時に読み込むものとすれば、パソコン通信機器を会員ユーザの住所または居所以外の場所に持ち出して接続しても、この個人認証システムは機能することとなる。

【００４２】なお、接続地域データＤ１を上記のようにして決めることもできるが、会員に直接入力してもらうこともできる。通信速度の関係で、アクセスポイントを電話料金が最も安いものとしない場合があるからである。

（第三の実施の形態）続いて、図４に基づいて第三の実施の形態について説明する。

【００４３】この第三の実施の形態は、個人認証システムが銀行のキャッシュカード１５による取引において採用される場合である。「会員データ」は接続地域データＤ１、すなわちキャッシュカード１５によって取引契約を行う銀行支店Ｂ１の所在地である。図４は、キャッシュカード１５によってキャッシュディスペンサー１６から現金を引き出す場合を説明している。

【００４４】キャッシュカード１５をキャッシュディスペンサー１６へ挿入し、暗証番号を入れたとすると、そのキャッシュディスペンサー１６は接続地域データＤ１をコンピュータセンターＢＢへ送る。一方、コンピュータセンターＢＢは、キャッシュカード１５の正規の持ち主のＰＨＳ端末装置２０の存在地域データＤ２をＰＨＳ事業者（ＰＰ）から取得し、接続地域データＤ１と存在地域データＤ２との一致を判断する。そして、一致していると判断すれば現金を引き出せ、一致していないと判断すれば引き出せないような出力結果を、キャッシュディスペンサー１６へ出力する。

（第四の実施の形態）続いて、図５に基づいて第四の実施の形態について説明する。

【００４５】この第四の実施の形態は、個人認証システムがクレジット会社ＣＣのクレジットカード１７による取引において採用される場合である。「会員データ」は接続地域データＤ１、すなわちクレジットカード１７が使用できるカード利用契約を結んだ商店Ｃ１の所在地である。図５は、クレジットカード１７によって商品を購入する際に、クレジットカード１７の有効期限などを照会するカードリーダー１８による読み込みの場合を説明している。

14

【００４６】カードリーダー１８によってクレジットカード１７の磁気情報が読み込まれたとすると、その情報は電話４（または専用回線）を介してクレジット会社ＣＣへ送る。一方、クレジット会社ＣＣは、カード契約データを読み込むとともに、クレジットカード１７の正規の持ち主のＰＨＳ端末装置２０の存在地域データＤ２をＰＨＳ事業者（ＰＰ）から取得し、接続地域データＤ１と存在地域データＤ２との一致を判断する。そして、一致していると判断すればそのクレジットカード１７が使用でき、一致していないと判断すればそのクレジットカード１７が使用できないとする出力結果を、カードリーダー１８へ出力する。

（第五の実施の形態）続いて、図６および図７に基づいて第五の実施の形態について説明する。この第五の実施の形態は、個人認証システムがクレジット会社ＣＣのクレジットカード１７による取引において採用される場合であって、第四の実施の形態の変形例である。

【００４７】第五の実施の形態が第四の実施の形態と異なるのは、クレジットカード１７の使用者が所有するはずのＰＨＳ端末装置２０へサービスデータを出力するというシステムを有する点である。更に詳しく説明する。第五の実施の形態は、存在地域データＤ２に対応する地域サービスデータを記憶する地域サービスデータ記憶手段、および地域サービスデータの内容をクレジットカード会員のＰＨＳ端末装置２０へ地域サービスデータＤ３を出力する地域サービスデータ出力手段を備えている。

【００４８】更に、カードリーダー１８には、ＰＨＳ端末装置２０と接続して地域サービスデータＤ３の出力があったかどうかの判断をする判断手段１９が備えられている。ここで「地域サービスデータＤ３」とは、ＰＨＳアンテナ基地局Ｐ１が位置する地域に関し、ＰＨＳ端末装置２０のユーザにとって有益な情報のことである。具体的には、買い物を済ませたユーザに対しての情報であるので、最寄り駅名、その最寄り駅の終電車時刻、当該クレジットカードが使用できる最寄りの商店のイベント情報などである。

【００４９】このような実施の形態にあっては、カード使用者が正規のクレジットカード会員であるとすると、手元のＰＨＳ端末装置２０から地域サービスデータＤ３を受け取り、そのことを判断手段１９が判断することによって、商店側はそのカード使用者が正規のクレジットカード会員であると判断できる。その後、取引契約を締

15

結すればよい。一方、カード使用者が正規のクレジットカード会員でないとすると、判断手段１９が手元のＰＨＳ端末装置２０から地域サービスデータＤ３を受け取れないと判断するはずであり、商店側はそのカード使用者が正規のクレジットカード会員でないと判断できる。クレジットカード１７のみを不正に取得した者がそのカード１７を使用している可能性が極めて高いからである。

（第六の実施の形態）続いて、図８に基づいて第六の実施の形態について説明する。

【００５０】この第六の実施の形態は、個人認証システムがクレジット会社ＣＣのクレジットカード１７による取引において採用される場合であって、第五の実施の形態の変形例である。第五の実施の形態と異なる点は、地域サービスデータＤ３を、商店Ｃ１が所有する機器、例えばカードリーダー１８に接続して設けたスピーカ１９Ａへ出力することとした点である。その出力が行われない、または商店Ｃ１の存在する地域にそぐわないものであれば、そのクレジットカード１７による取引を中止する。

【００５１】上記してきた第一ないし第六の実施の形態において個人認証のために会員ユーザに要求されることは、ＰＨＳ端末装置２０を手元に置いておくことのみであり、新たに暗証番号を覚えたり、新しい鍵を持ち歩いたりすることを強いるものではない。

（第七の実施の形態）続いて、図９および図１０に基づいて第七の実施の形態について説明する。

【００５２】この第七の実施の形態は、個人認証システムがクレジット会社ＣＣのクレジットカード１７による取引において採用される場合であって、構成をシンプル化し、更にＰＨＳ端末装置だけではなく、ポケットベルや通常の携帯電話も使用できるようにした個人認証のためのシステムである。この第七の実施の形態は、会員ユーザのＰＨＳ端末装置２０の電話番号を予めデータベースに記憶している。そして、取引をしようとする会員ユーザのクレジットカード１７をカードリーダー１８で読み、会員ユーザの接続地域データＤ１を商店Ｃ１の電話１４など通信回線から取得する。接続地域データＤ１を取得したクレジットカード会社ＣＣは、データベースに記憶された会員ユーザの電話番号を読み込み、ＰＨＳ端末装置２０へ認証のための電話をかける。

【００５３】会員ユーザのＰＨＳ端末装置２０に認証のための電話がクレジットカード会社ＣＣからかかってくれば、店員はその電話がかかってきたことで、目の前の会員ユーザが正規の会員であると推定して取引を成立させればよい。認証コールがなければ、目の前の会員ユーザが正規の会員でないかもしれないと推定し、カードでの取引ができない旨を伝えればよい。

【００５４】なお、この実施の形態では携帯通信端末としてＰＨＳ端末装置２０を採用したが、ポケットベルや通常の携帯電話でもよい。第七の実施の形態において個

16

人認証のために会員ユーザに要求されることは、クレジットカード会社ＣＣにデータ登録した携帯通信端末装置（この例においてはＰＨＳ端末装置２０）を手元に置いておくことのみであり、新たに暗証番号を覚えたり、新しい鍵を持ち歩いたりすることを強いるものではない。

【００５５】

【発明の効果】請求項１ないし請求項３および請求項９記載の発明によれば、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証システムを提供することができた。請求項４記載の発明によれば、更に、不正なアクセス者に不利益を被らせるようなシステムとすることによって、結果的に不正なアクセス者を未然防止できる個人認証システムを提供することができた。

【００５６】請求項５記載および請求項１０によれば、正規の会員ユーザが持つべき認証情報を過度に複雑化することなく、会員ユーザにこれまで以上の余計な操作を強いない個人認証方法を提供することができた。請求項６および請求項７記載の発明によれば、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証システムを提供することができた。

【００５７】請求項８記載の発明によれば、正規のクレジットカード会員が持つべき認証情報を過度に複雑化することなく、カード会員にこれまで以上の余計な操作を強いない個人認証方法を提供することができた。

【図面の簡単な説明】

【図１】本発明の第一の実施の形態を示す概念図である。

【図２】本発明の第一の実施の形態を示すフローチャートである。

【図３】本発明の第二の実施の形態を示す概念図である。

【図４】本発明の第三の実施の形態を示す概念図である。

【図５】本発明の第四の実施の形態を示す概念図である。

【図６】本発明の第五の実施の形態を示す概念図である。

【図７】本発明の第五の実施の形態を示すフローチャートである。

【図８】本発明の第六の実施の形態を示す概念図である。

【図９】本発明の第七の実施の形態を示す概念図である。

【図１０】本発明の第七の実施の形態を示すフローチャートである。

【符号の説明】

１０　　通信接続手段

17

１２　パソコン
ム
１４　電話
ッシュカード
１６　キャッシュディスペンサー
ジットカード
１８　カードリーダー
１９　判断手段
ーカ
２０　ＰＨＳ端末装置
ＡＡ　パソコン通信事業者

１３　モデ

１５　キャ

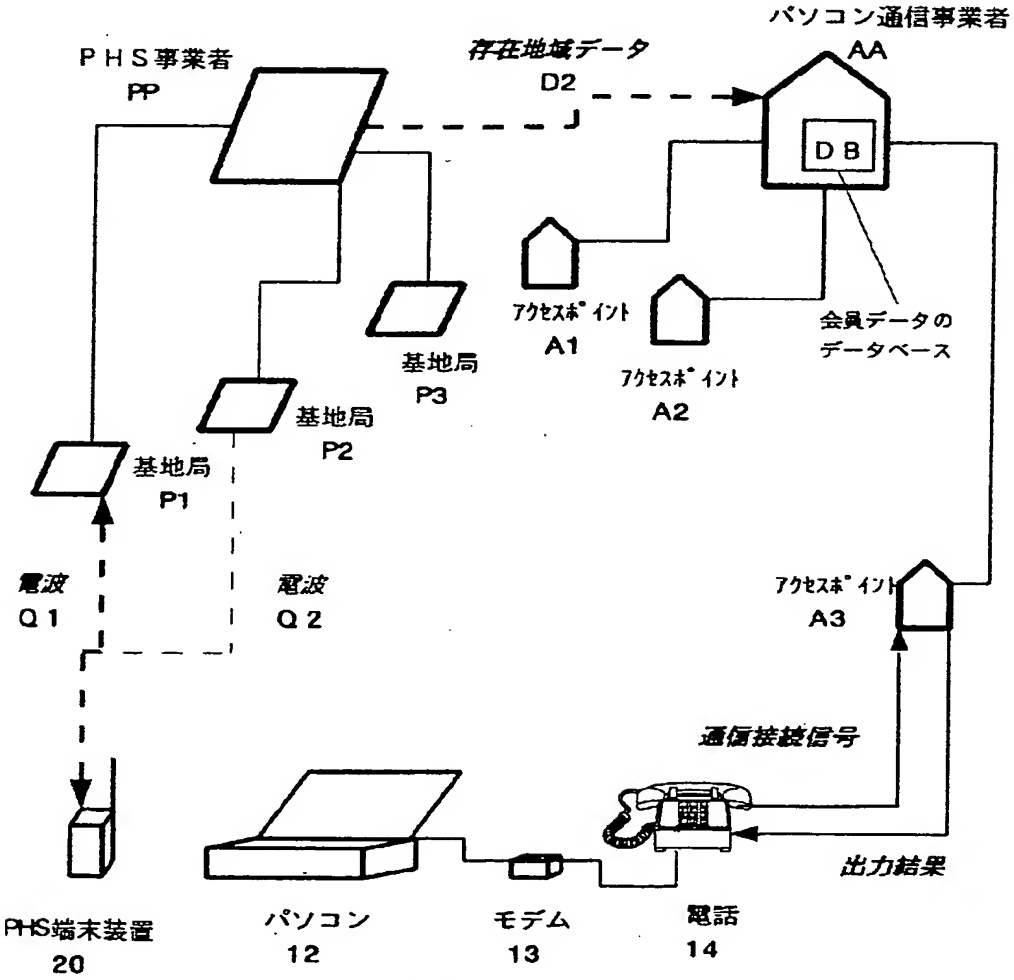
１７　クレ

１９Ａ　スピ

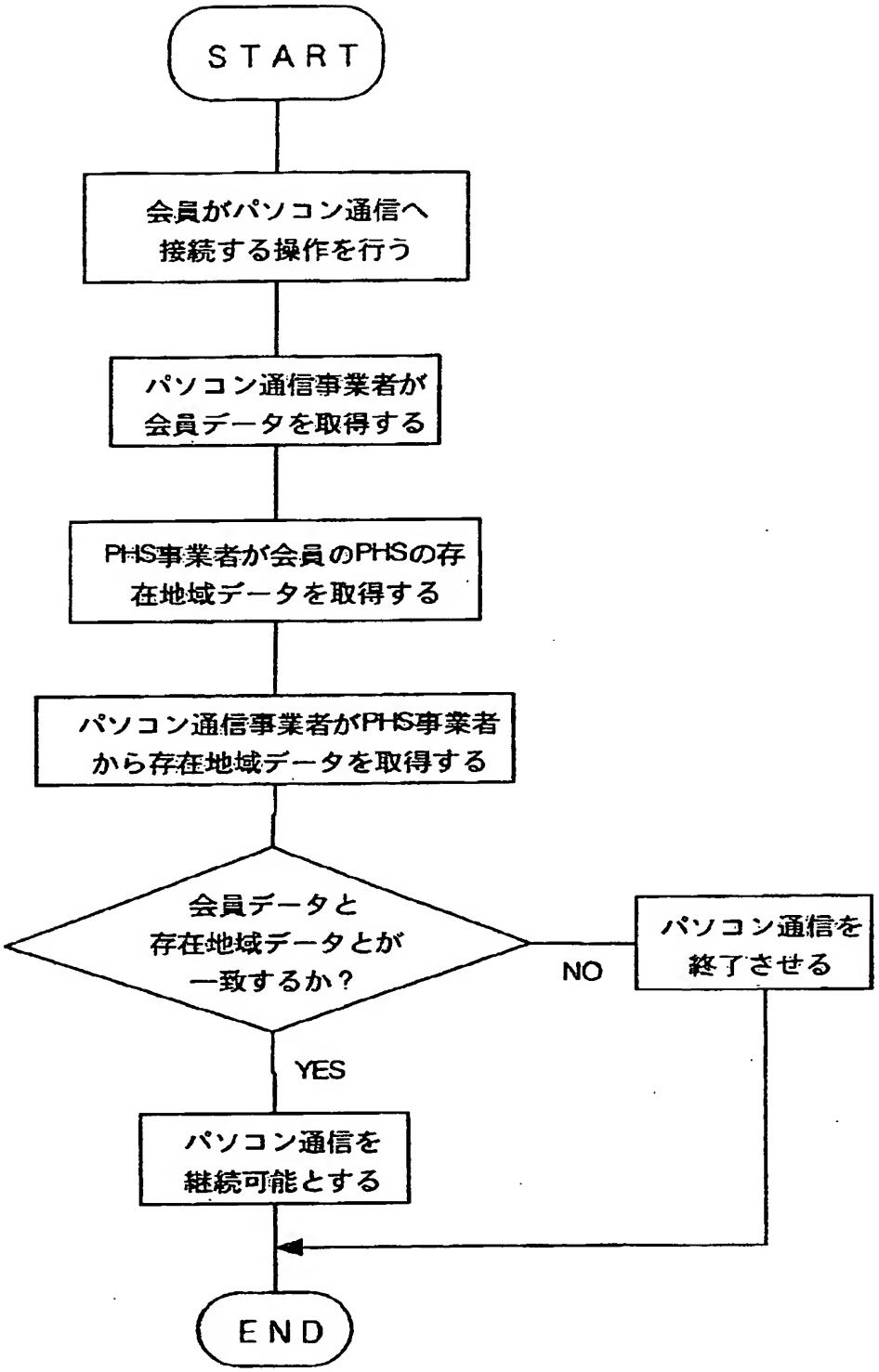
18

Ａ１，Ａ２，Ａ３　アクセスポイント
ＢＢ　銀行が管理するコンピュータセンター
Ｂ１　銀行支店
ＣＣ　クレジット会社
Ｃ１　商店
Ｄ１　接続地域データ　　Ｄ２　存在
地域データ
Ｄ３　地域サービスデータ
ＰＰ　ＰＨＳ事業者
10　Ｐ１，Ｐ２，Ｐ３　基地局
Ｑ１，Ｑ２　電波

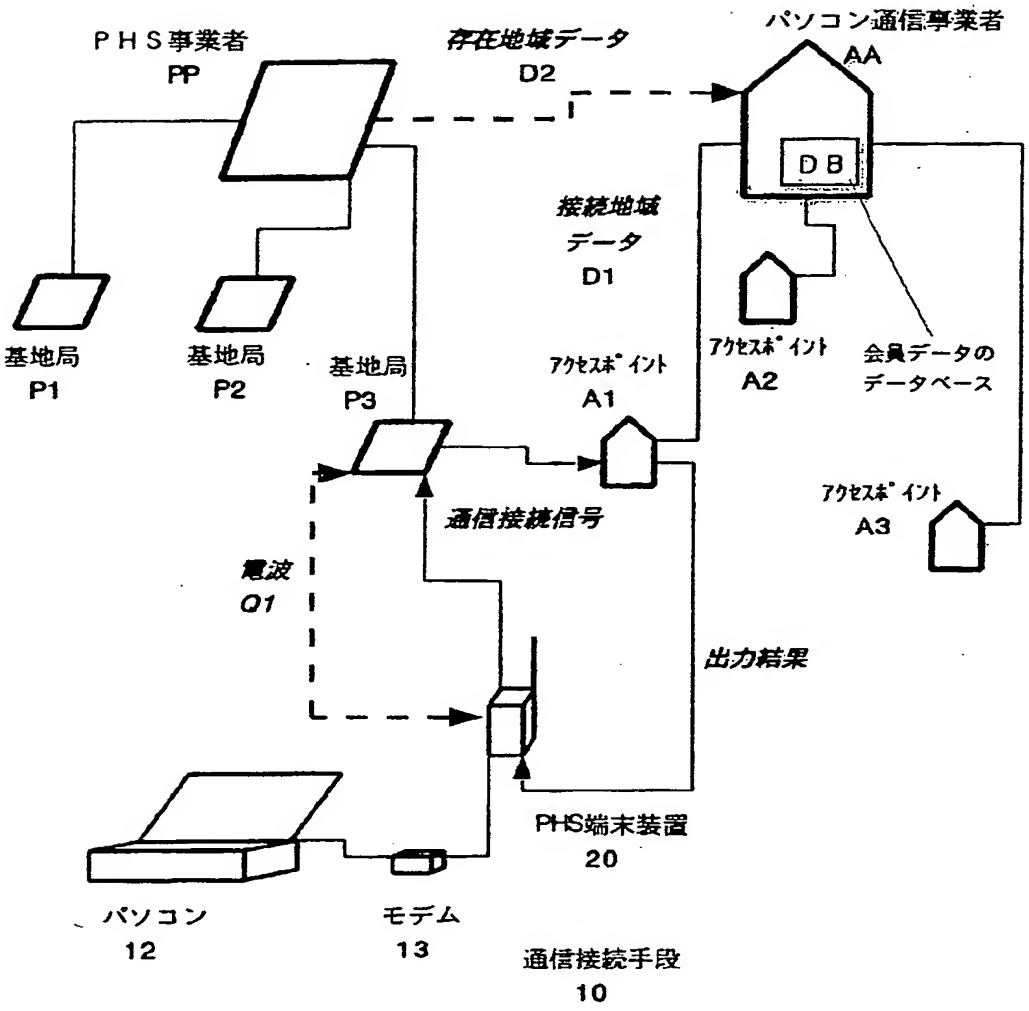
【図１】



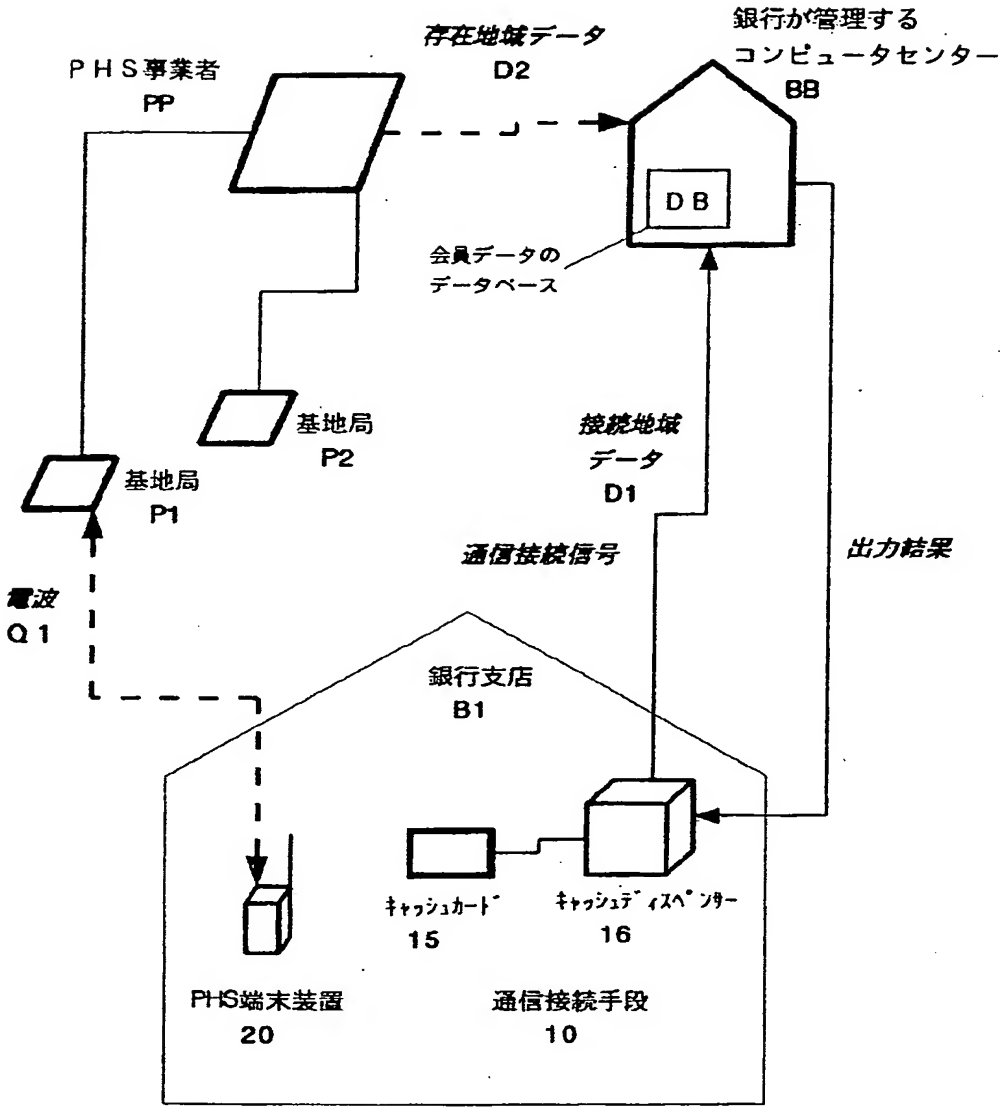
【図２】


START
会員がパソコン通信へ接続する操作を行う
パソコン通信事業者が会員データを取得する
PHS事業者が会員のPHSの存在地域データを取得する
パソコン通信事業者がPHS事業者から存在地域データを取得する
会員データと存在地域データとが一致するか？
NO
パソコン通信を終了させる
YES
パソコン通信を継続可能とする
END

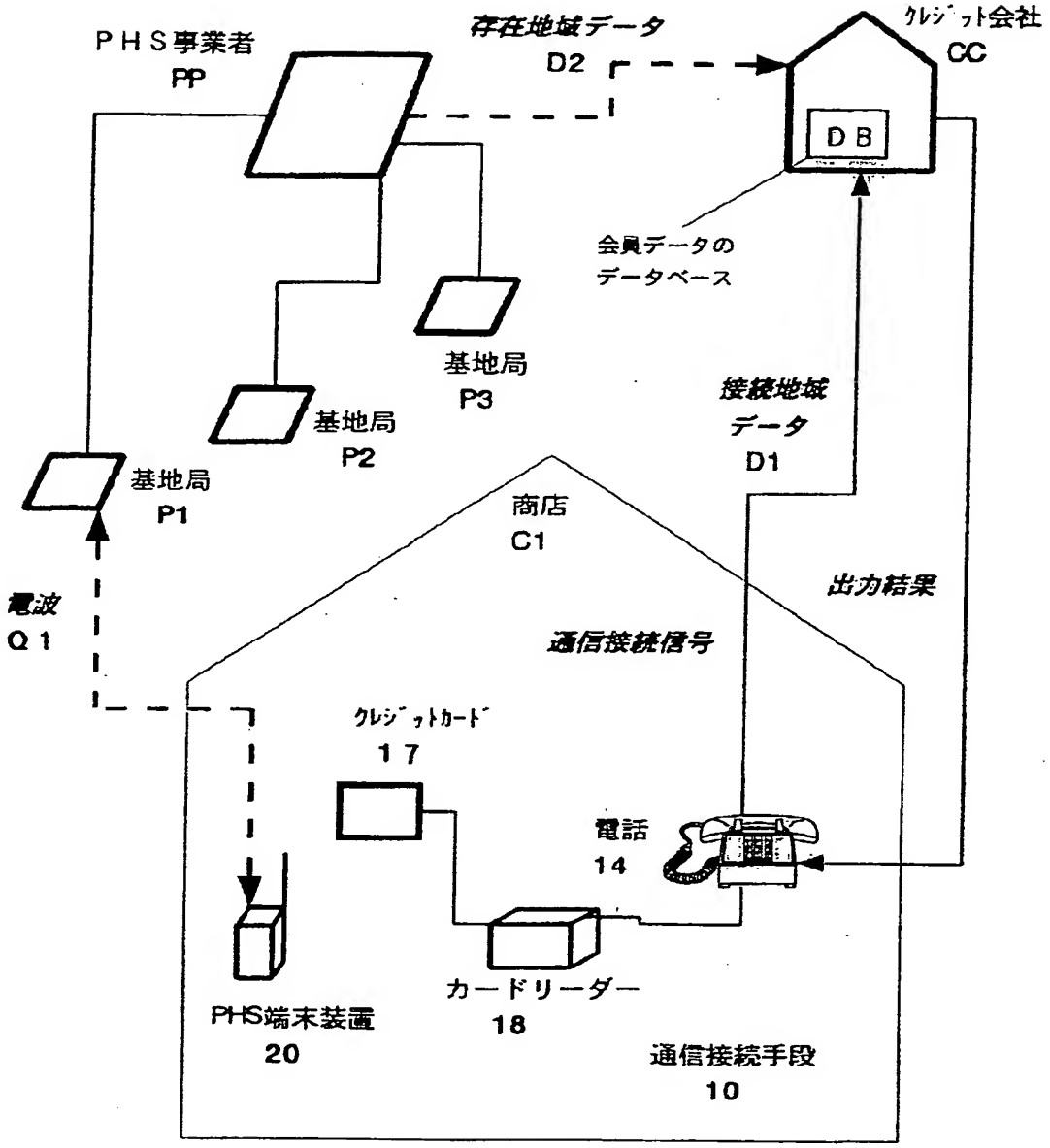
【図３】


ＰＨＳ事業者
PP
存在地域データ
D2
パソコン通信事業者
AA
ＤＢ
接続地域
データ
D1
基地局
P1
基地局
P2
基地局
P3
ｱｸｾｽﾎﾟｲﾝﾄ
A1
ｱｸｾｽﾎﾟｲﾝﾄ
A2
会員データの
データベース
ｱｸｾｽﾎﾟｲﾝﾄ
A3
通信接続信号
電波
Q1
出力結果
PHS端末装置
20
パソコン
12
モデム
13
通信接続手段
10

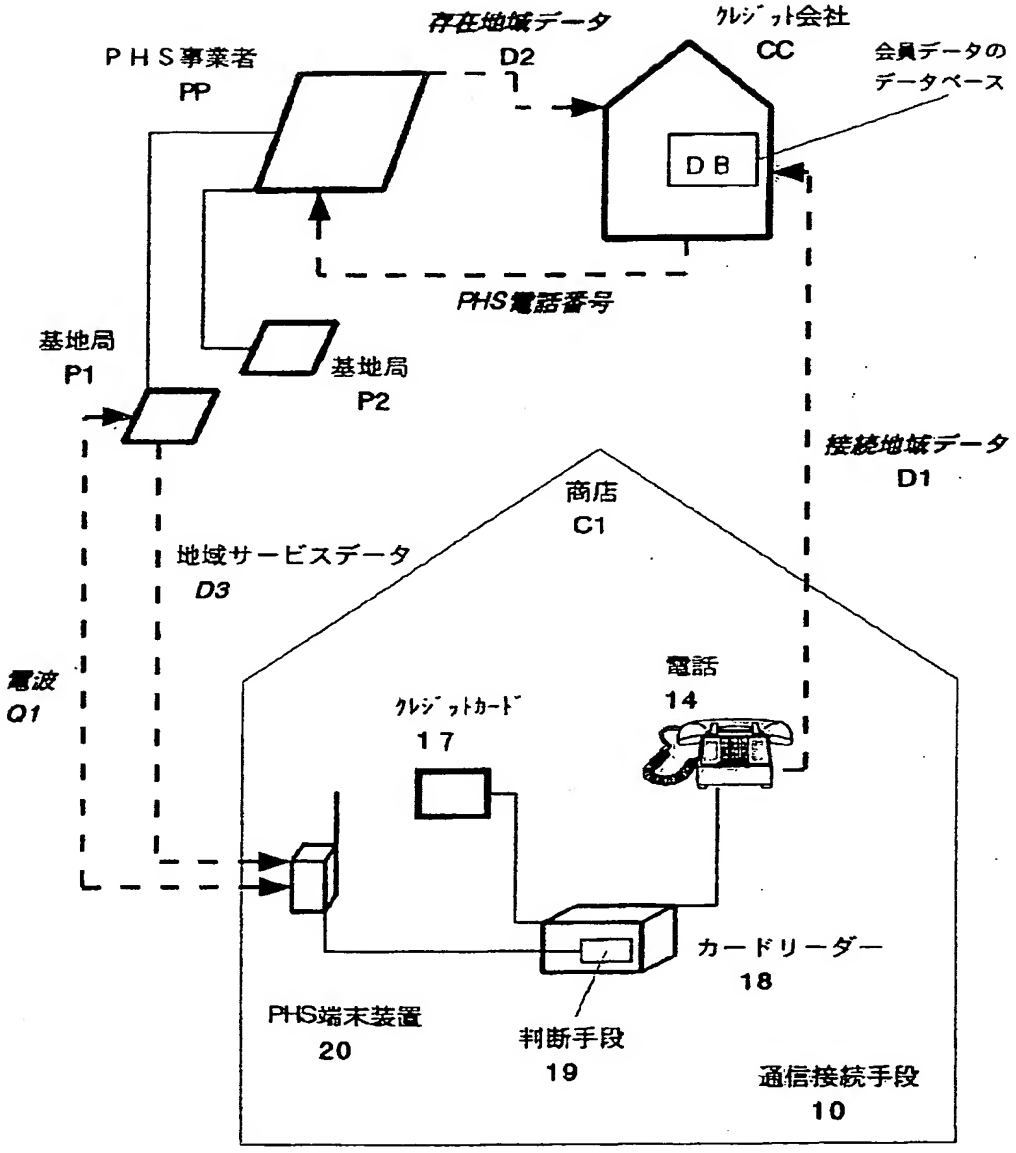
【図４】


銀行が管理する
コンピュータセンター
BB
存在地域データ
D2
ＰＨＳ事業者
PP
ＤＢ
会員データの
データベース
基地局
P2
基地局
P1
接続地域
データ
D1
通信接続信号
出力結果
電波
Q1
銀行支店
B1
キャッシュカード
15
キャッシュディスペンサー
16
PHS端末装置
20
通信接続手段
10

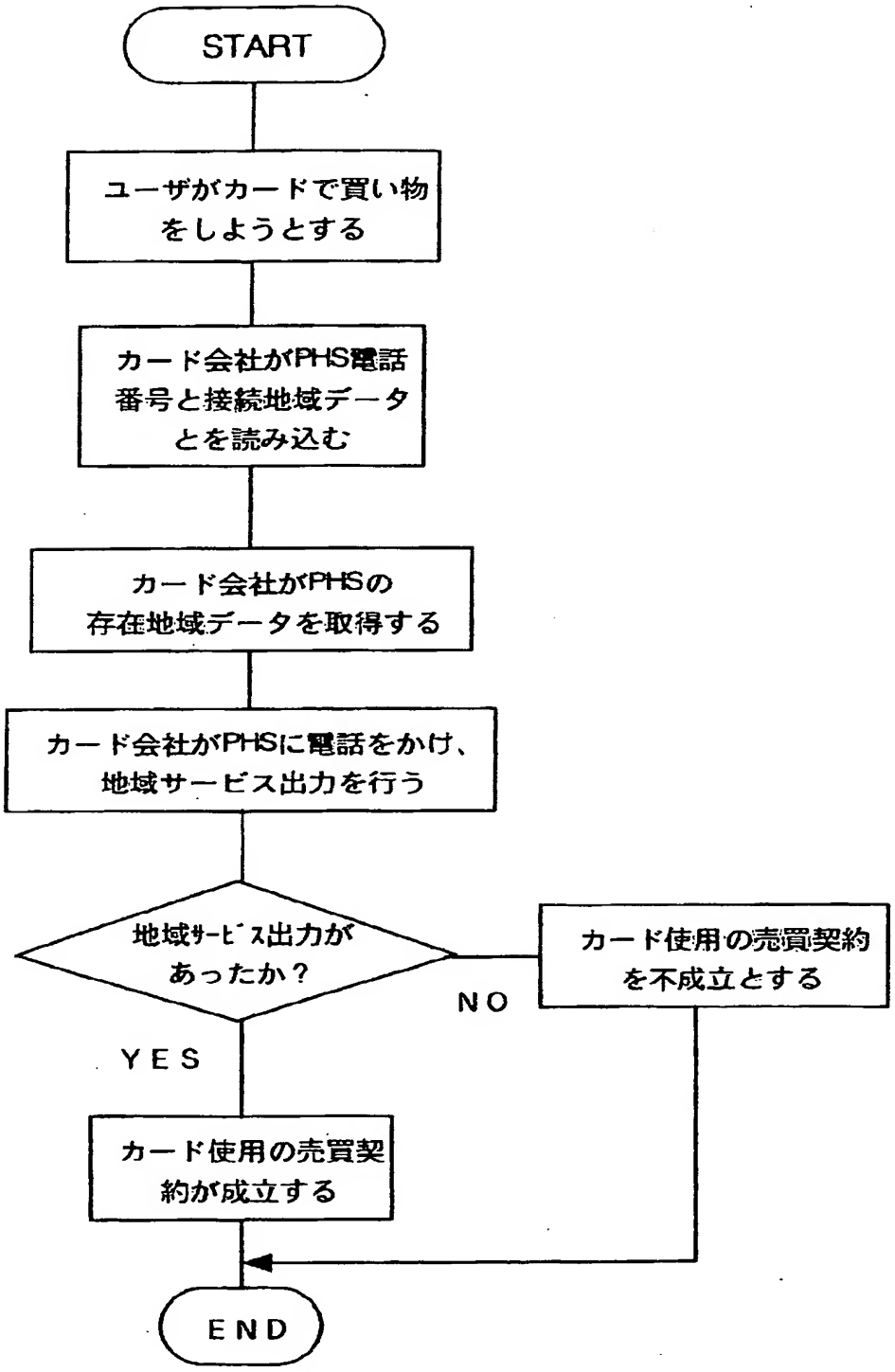
【図５】


ＰＨＳ事業者
PP
存在地域データ
D2
ｸﾚｼﾞｯﾄ会社
CC
ＤＢ
会員データの
データベース
基地局
P3
基地局
P2
基地局
P1
接続地域
データ
D1
商店
C1
出力結果
電波
Q1
通信接続信号
ｸﾚｼﾞｯﾄｶｰﾄﾞ
17
電話
14
PHS端末装置
20
カードリーダー
18
通信接続手段
10

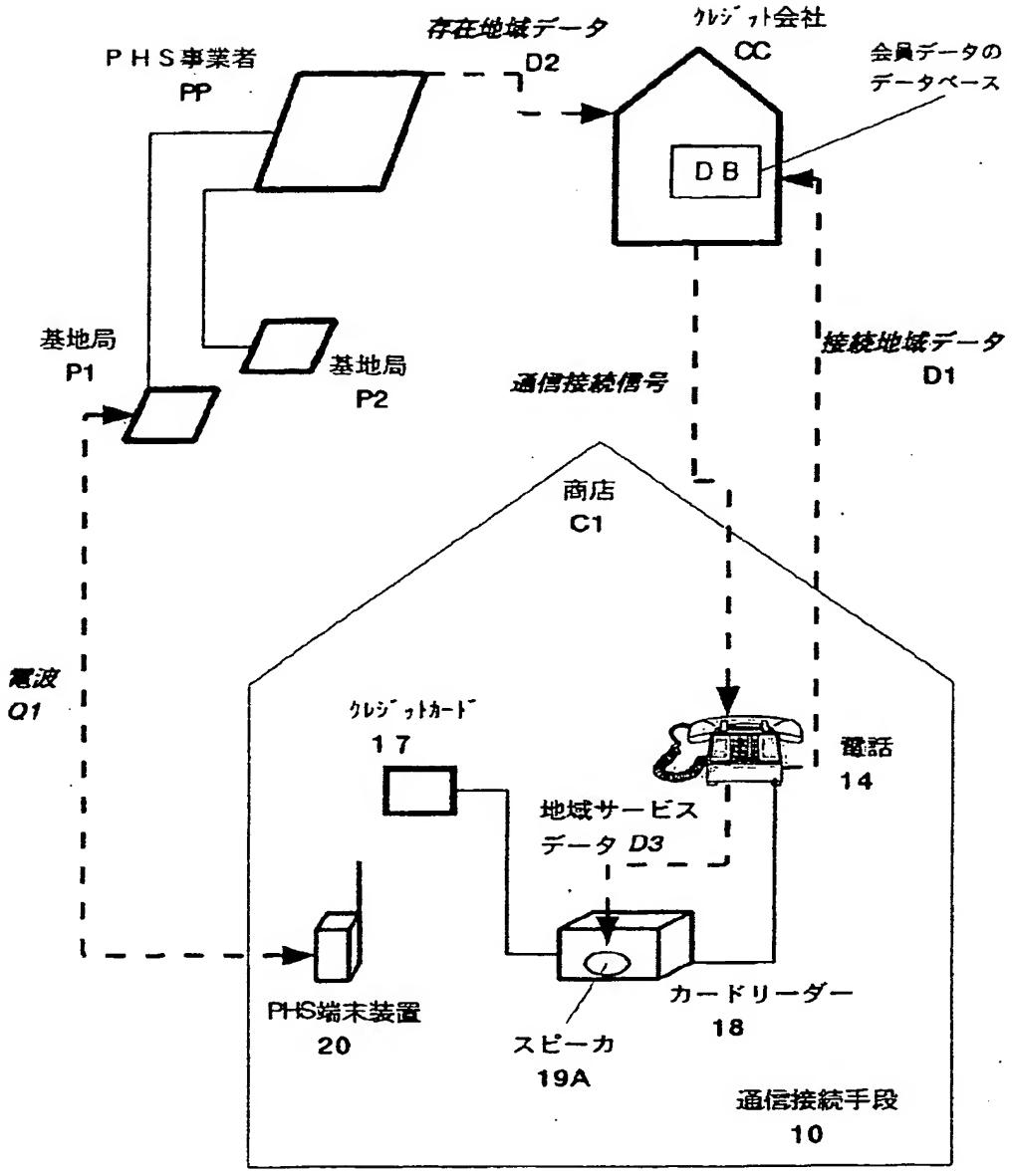
【図６】


存在地域データ
D2
ｸﾚｼﾞｯﾄ会社
CC
ＰＨＳ事業者
PP
会員データの
データベース
ＤＢ
PHS電話番号
基地局
P1
基地局
P2
接続地域データ
D1
商店
C1
地域サービスデータ
D3
電波
Q1
電話
14
ｸﾚｼﾞｯﾄｶｰﾄﾞ
17
カードリーダー
18
PHS端末装置
20
判断手段
19
通信接続手段
10

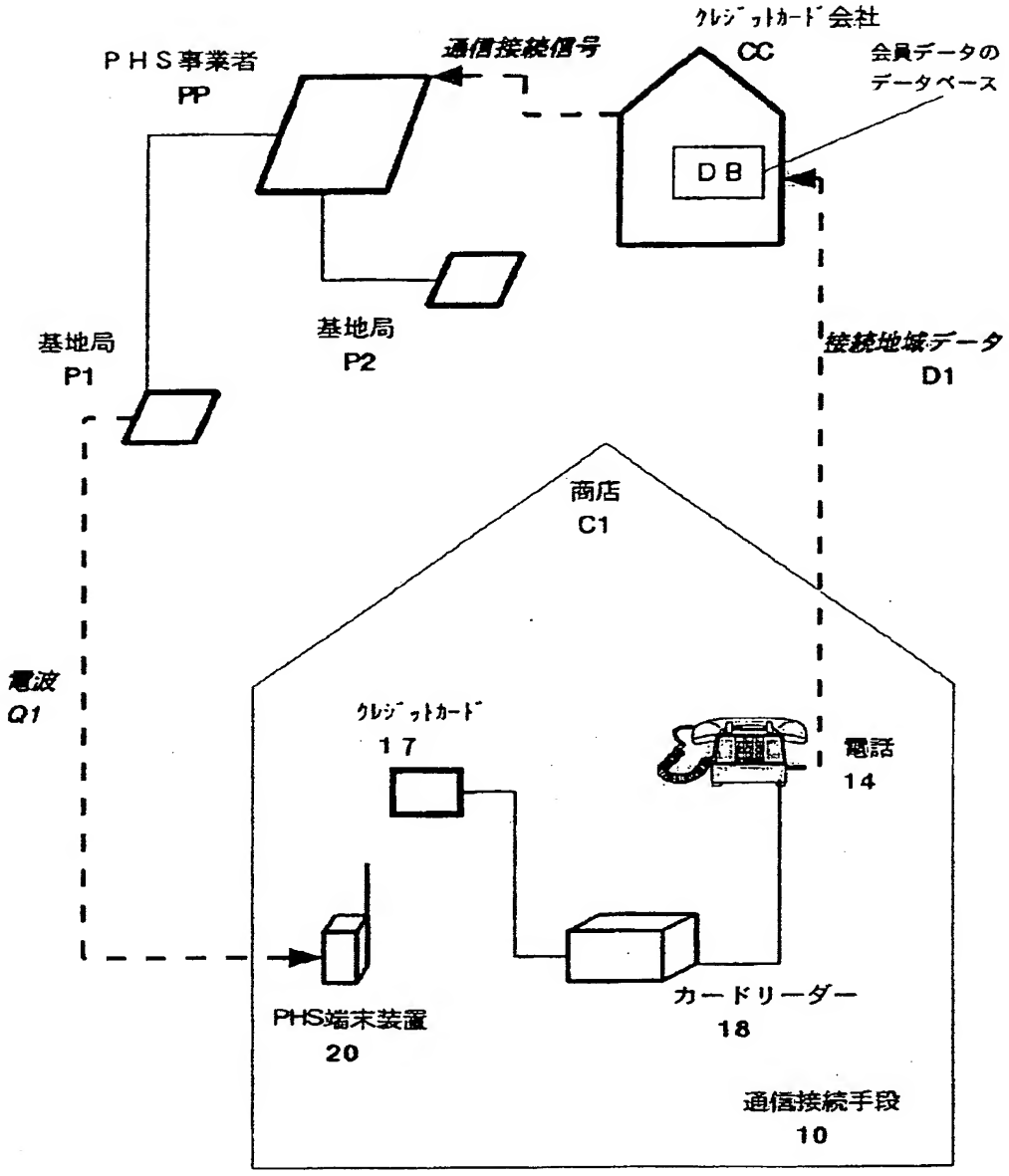
【図７】


START
ユーザがカードで買い物をしようとする
カード会社がPHS電話番号と接続地域データとを読み込む
カード会社がPHSの存在地域データを取得する
カード会社がPHSに電話をかけ、地域サービス出力を行う
地域ｻｰﾋﾞｽ出力があったか？
NO
カード使用の売買契約を不成立とする
YES
カード使用の売買契約が成立する
END

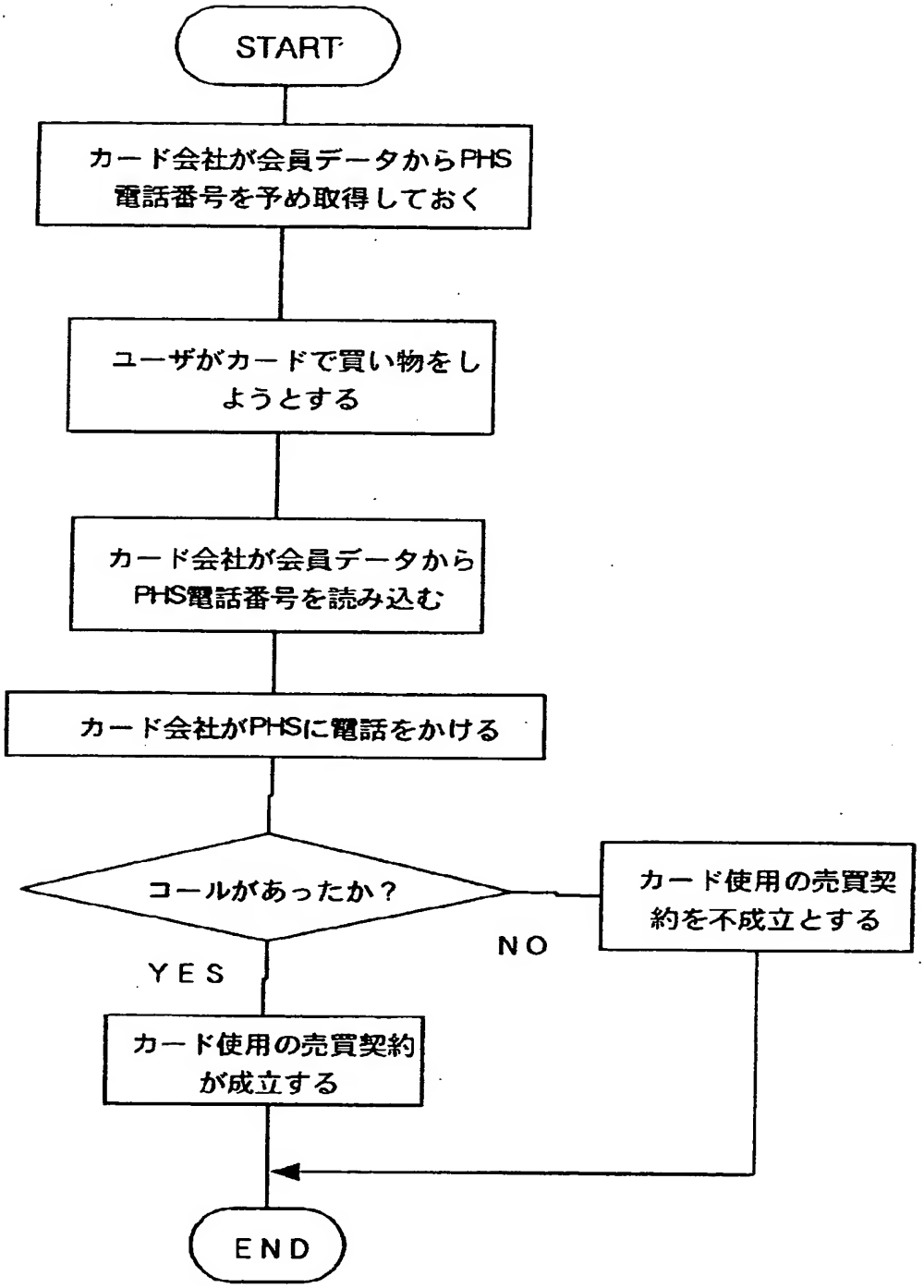
【図８】


存在地域データ
D2
ｸﾚｼﾞｯﾄ会社
CC
会員データの
データベース
ＰＨＳ事業者
PP
ＤＢ
基地局
P1
基地局
P2
通信接続信号
接続地域データ
D1
商店
C1
電波
Q1
ｸﾚｼﾞｯﾄｶｰﾄﾞ
17
電話
14
地域サービス
データ D3
PHS端末装置
20
カードリーダー
18
スピーカ
19A
通信接続手段
10

【図９】


ｸﾚｼﾞｯﾄｶｰﾄﾞ会社
CC
通信接続信号
ＰＨＳ事業者
PP
会員データの
データベース
ＤＢ
基地局
P2
基地局
P1
接続地域データ
D1
商店
C1
電波
Q1
ｸﾚｼﾞｯﾄｶｰﾄﾞ
17
電話
14
PHS端末装置
20
カードリーダー
18
通信接続手段
10

【図１０】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04M 3/42		H04B 7/26	109B